Bitdefender®

INTERNET SECURITY 2015

MANUAL DO UTILIZADOR

Bitdefender Internet Security 2015
Manual do Utilizador

Editado 10/21/2014

Copyright© 2014 Bitdefender

Aviso Legal

Todos os direitos reservados. Nenhuma parte deste livro pode ser reproduzida ou transmitida de qualquer forma ou por quaisquer meios, eletrónicos ou mecânicos, incluindo fotocópias, gravação, ou qualquer sistema de arquivo de informação, sem a permissão por escrito de um representante autorizado de Bitdefender. A inclusão de pequenas frases do texto em comparativas poderão ser feitas desde que seja feita a menção da fonte da frase em questão. O conteúdo não pode ser de forma alguma modificado.

Aviso e Renúncia. Este produto e a sua documentação estão protegidas por direitos de autor. A informação neste documento é apresentada numa base de "tal como é", sem qualquer garantia. Apesar de todas as precauções terem sido tomadas na preparação deste documento, os autores não serão responsabilizados por qualquer pessoa ou entidade com respeito a qualquer perda ou dano causado ou alegadamente causado directa ou indirectamente pela informação contida neste livro.

Este livro contém links para Websites de terceiras partes que não estão baixo controlo da Bitdefender, e a Bitdefender não é responsável pelo conteúdo de qualquer site acedido por link. Se aceder a um site de terceiras partes mencionado neste manual, faz isso à sua própria conta e risco. A Bitdefender fornece esses links apenas para facilitar, e a inclusão do link não implica que a Bitdefender endosse ou aceite qualquer responsabilidade pelo conteúdo deste sites de terceiras partes.

Marcas Registadas. Nomes de Marcas Registadas poderão aparecer neste livro. Todas as marcas registadas ou não registadas neste documento são da exclusiva propriedade dos seus respetivos proprietários.

Bitdefender

Índice

Instalação 1
1. A preparar a instalação 2
2. Requisitos do sistema 3
2.1. Requisitos mínimos do sistema 3
2.2. Requisitos de sistema recomendados 3
2.3. Requisitos de Software 4
3. Instalação do seu produto Bitdefender 5
Introdução 11
4. Os básicos 12
4.1. A abrir a janela do Bitdefender 13
4.2. A reparar problemas 13
4.2.1. Assistente Reparar Todas as Incidências 14
4.2.2. Configurar os alertas de estado 15
4.3. Eventos 15
4.4. Autopilot 17
4.5. Perfis e Modo de Bateria 18
4.5.1. Perfis 18
4.5.2. Modo de Bateria 19
4.6. Definições de proteção da palavra-passe de Bitdefender 21
4.7. Relatórios anónimos de utilização 22
4.8. Ofertas especiais e notificações de produto 22
5. Interface Bitdefender 24
5.1. Ícone na área de notificação 24
5.2. Janela Principal 25
5.2.1. Barra de ferramentas superior 26
5.2.2. Área de painéis 27
5.3. Os módulos do Bitdefender 32
5.4. Dispositivo de Segurança 33
5.4.1. Analisar ficheiros e pastas 34
5.4.2. Ocultar / mostrar Dispositivo de Segurança 34
5.5. Relatório de Segurança 35
5.5.1. A verificar o Relatório de Segurança 37
5.5.2. Ativar ou desativar a notificação do Relatório de Segurança 38
6. A registar o Bitdefender 39
6.1. Inserir a sua chave de licença 39
6.2. Adquirir ou renovar chaves de licença 40
7. Conta MyBitdefender 41
7.1. Ligar o seu computador à MyBitdefender 41
8. Mantenha o seu Bitdefender atualizado. 44
8.1. Verifique se o Bitdefender está atualizado 45

8.2. A efetuar uma atualização ... 45
8.3. Ligar ou desligar a atualização automática ... 45
8.4. Ajuste das configurações da atualização ... 46

Como ... 48

9. Instalação ... 49
9.1. Como instalo o Bitdefender num segundo computador? ... 49
9.2. Quando é que devo reinstalar o Bitdefender? ... 49
9.3. Onde posso transferir o meu produto Bitdefender? ... 50
9.4. Como posso mudar de um produto Bitdefender para outro? ... 50
9.5. Como utilizo a minha chave de licença do Bitdefender após a atualização do Windows? ... 51
9.6. Como reparo o Bitdefender? ... 54

10. Registo ... 55
10.1. Que produto Bitdefender estou a usar? ... 55
10.2. Como posso registar uma versão teste? ... 55
10.3. Quando é que a proteção do Bitdefender expira? ... 55
10.4. Como posso renovar a proteção do meu Bitdefender? ... 56

11. MyBitdefender ... 58
11.1. Como inicio sessão na MyBitdefender utilizando outra conta online? ... 58
11.2. Como altero o endereço de e-mail utilizado para a conta MyBitdefender? ... 58
11.3. Como reponho a palavra-passe da conta MyBitdefender? ... 59

12. A analisar com Bitdefender ... 61
12.1. Como posso analisar um ficheiro ou uma pasta? ... 61
12.2. Como posso analisar o seu sistema? ... 61
12.3. Como posso criar uma tarefa de análise personalizada? ... 62
12.4. Como posso excluir uma pasta da análise? ... 62
12.5. O que fazer se o Bitdefender identificar um ficheiro limpo como infectado? ... 63
12.6. Como posso saber que vírus o Bitdefender detetou? ... 64

13. Controlo Parental ... 66
13.1. Como posso proteger os meus filhos de ameaças online? ... 66
13.2. Como posso restringir o acesso à Internet do meu filho? ... 67
13.3. Como bloqueio o acesso do meu filho a um website? ... 67
13.4. Como impeço o meu filho de jogar um jogo? ... 68
13.5. Como posso criar contas de utilizador do Windows? ... 69
13.6. Como remover um perfil de criança ... 70

14. Protecção de Privacidade ... 71
14.1. Como posso ter a certeza de que a minha transação online é segura? ... 71
14.2. Como protejo a minha conta do Facebook? ... 71
14.3. Como protejo a minha informação pessoal? ... 72
14.4. Como removo um ficheiro permanentemente com o Bitdefender? ... 72

15. TuneUp ... 73
15.1. Como posso usar melhorar o desempenho do meu sistema? ... 73
15.1.1. Desfragmente o seu disco rígido ... 73
15.1.2. Otimize o desempenho do seu sistema com um único clique ... 73

15.1.3. Analise o seu sistema periodicamente ... 74
15.2. Como posso melhorar o tempo de arranque do meu sistema? ... 74

16. Informações Úteis ... 76
16.1. Como testo a minha solução antivírus? ... 76
16.2. Como posso remover o Bitdefender? ... 76
16.3. Como mantenho o meu sistema protegido após a desinstalação do Bitdefender? ... 78
16.4. Como desligo automaticamente o meu computador após terminar a análise? ... 79
16.5. Como posso configurar Bitdefender para usar um proxy de ligação à Internet? ... 80
16.6. Estou a utilizar uma versão de 32 ou 64 Bit do Windows? ... 81
16.7. Como posso mostrar objetos ocultos no Windows? ... 82
16.8. Como posso remover outras soluções de segurança? ... 83
16.9. Como posso usar o Restauro do Sistema no Windows? ... 84
16.10. Como posso reiniciar no Modo de Segurança? ... 85

Gerir a sua segurança ... 86

17. Proteção Antivírus ... 87
17.1. Análise no acesso (proteção em tempo real) ... 88
17.1.1. Ligar ou desligar a proteção em tempo real ... 88
17.1.2. Ajustar o nível de proteção em tempo real ... 89
17.1.3. Configurar as definições da proteção em tempo-real ... 89
17.1.4. Restaurar as predefinições ... 93
17.2. Verificação por ordem ... 94
17.2.1. Procurar malware num ficheiro ou pasta ... 94
17.2.2. Executar uma Análise Rápida ... 94
17.2.3. Executar uma Análise do Sistema ... 95
17.2.4. Configurar uma análise personalizada ... 96
17.2.5. Assistente de Análise Antivírus ... 99
17.2.6. Ver os relatórios da análise ... 102
17.3. Análise automática de média removíveis ... 103
17.3.1. Como funciona? ... 103
17.3.2. Gerir análise de média removível ... 104
17.4. Configurar exceções da análise ... 105
17.4.1. Excluir pastas e ficheiros da análise ... 105
17.4.2. Excluir extensões de ficheiros da análise ... 106
17.4.3. Gerir exceções da análise ... 107
17.5. Gerir ficheiros da quarentena ... 107
17.6. Controlo Ativo de Vírus ... 108
17.6.1. Verificar aplicações detetadas ... 109
17.6.2. Ligar ou desligar o Controlo Ativo de Vírus ... 109
17.6.3. Ajustar proteção de Controlo de Vírus Ativo ... 110
17.6.4. Gerir processos excluídos ... 110

18. Antispam ... 112
18.1. Compreender o Antispam ... 113
18.1.1. Filtros impeditivos da entrada de mails indesejados ... 113

18.1.2. Operação Antispam ... 113
18.1.3. Clientes de email e protocolos suportados ... 114
18.2. Ligar ou desligar a proteção antispam ... 114
18.3. Utilizar a barra de ferramentas Antispam na janela do seu cliente de email ... 114
18.3.1. Indicar os erros de deteção ... 116
18.3.2. Indicar mensagens de spam não detetadas ... 116
18.3.3. Configurar definições da barra de ferramentas ... 116
18.4. Configurar a Lista de Amigos ... 117
18.5. Configurar a lista de Spammers ... 118
18.6. A configurar os filtros locais Antispam ... 120
18.7. Configurar as definições da nuvem ... 120

19. Proteção da Internet ... 122
19.1. Proteção do Bitdefender no navegador da web ... 123
19.2. Alertas de Bitdefender no navegador ... 125

20. Proteção de dados ... 126
20.1. Acerca da proteção de dados ... 126
20.2. Configurar proteção de dados ... 126
20.2.1. Criar regras de proteção de dados ... 127
20.3. Gerir regras ... 128
20.4. Apagar ficheiros permanentemente ... 128

21. Vulnerabilidade ... 130
21.1. Procurar vulnerabilidades no seu sistema ... 130
21.2. Usar monitorização de vulnerabilidade automática ... 131

22. Firewall ... 134
22.1. Ativar/desativar firewall de proteção ... 134
22.2. Gerir regras da Firewall ... 135
22.2.1. Regras gerais ... 135
22.2.2. Regras da aplicação ... 136
22.3. Gerir definições da ligação ... 139
22.4. Configurar definições avançadas ... 141
22.5. Configurar intensidade de alertas ... 141

23. Deteção de Intrusão ... 143

24. Segurança Safepay para transações online ... 144
24.1. A utilizar o Bitdefender Safepay™ ... 145
24.2. Configurar definições ... 146
24.3. Gerir bookmarks ... 147
24.4. Proteção Hotspot em redes não-seguras. ... 147

25. Proteção de Carteira para as suas credenciais ... 149
25.1. Configurar a Carteira ... 150
25.2. Ligar ou desligar a proteção da Carteira ... 152
25.3. Gerir as definições da Carteira ... 152

26. Controlo Parental ... 156
26.1. Aceder ao Painel do Controlo Parental ... 156
26.2. Adicionar o perfil do seu filho ... 157

26.2.1. Instalar o Controlo Parental no dispositivo Android ... 158
26.2.2. Monitorizar a atividade da criança ... 159
26.2.3. Configurar as Definições Gerais ... 159
26.3. Configurar Controlo Parental ... 160
26.3.1. Controlo Web ... 161
26.3.2. Controlo de Aplicações ... 163
26.3.3. Proteção Facebook ... 164
26.3.4. Controlo de Mensagens Instantâneas ... 165
26.3.5. Localização ... 165
26.3.6. Controlo de mensagens de texto ... 166
26.3.7. Controlo de números de telefone ... 167
27. Proteção Safego para o Facebook ... 168
28. Bitdefender USB Immunizer ... 170
29. Gerir os seus computadores remotamente ... 171
29.1. A aceder à MyBitdefender ... 171
29.2. Executar tarefas nos computadores ... 171
Otimização do sistema ... 173
30. TuneUp ... 174
30.1. A otimizar a velocidade do seu sistema com apenas um clique ... 174
30.2. A otimizar o tempo de arranque do seu PC. ... 175
30.3. Limpeza do seu PC ... 177
30.4. Desfragmentar volumes de discos rígidos ... 178
30.5. Limpar o registo do Windows ... 179
30.6. Recuperar registo limpo ... 180
30.7. Localizar ficheiros duplicados ... 181
31. Perfis ... 183
31.1. Perfil Trabalho ... 184
31.2. Perfil de Filme ... 185
31.3. Perfil de jogo ... 186
31.4. Otimização em Tempo Real ... 187
Solução de problemas ... 189
32. Resolver incidências comuns ... 190
32.1. O meu sistema parece estar lento ... 190
32.2. A análise não inicia ... 192
32.3. Já não consigo usar uma aplicação ... 194
32.4. O que fazer quando o Bitdefender bloqueia um site Web ou uma aplicação online segura ... 195
32.5. Não consigo ligar à Internet ... 196
32.6. Não consigo aceder a um dispositivo na minha rede ... 197
32.7. A minha Internet está lenta ... 199
32.8. Como atualizar o Bitdefender numa ligação à Internet lenta ... 201
32.9. O Meu Computador não está ligado à Internet. Como posso actualizar o Bitdefender? ... 201

32.10. Os serviços Bitdefender não estão a responder 202
32.11. O filtro Antispam não está a funcionar corretamente 203
32.11.1. Mensagens legítimas são marcadas como [spam] 203
32.11.2. Muitas mensagens de spam não são detetadas 205
32.11.3. O Filtro Antispam não deteta nenhuma mensagem spam 206
32.12. A funcionalidade Preenchimento automático na minha Carteira não funciona 207
32.13. Remoção de Bitdefender falhou 208
32.14. O meu sistema não reinicia após a instalação de Bitdefender 210

33. Remover malware do seu sistema 215
33.1. Modo de Recuperação Bitdefender 215
33.2. O que fazer se o Bitdefender encontrar vírus no seu computador? 218
33.3. Como posso limpar um vírus num ficheiro? 219
33.4. Como posso limpar um vírus num ficheiro do email? 220
33.5. O que fazer se suspeitar que um ficheiro é perigoso? 221
33.6. Como limpar ficheiros infectados da Informação de Volume do Sistema 222
33.7. O que são os ficheiros protegidos por palavra-passe no relatório de análise? 224
33.8. O que são os itens ignorados no relatório de análise? 224
33.9. O que são os ficheiros muito comprimidos no relatório de análise? 224
33.10. Por que é que Bitdefender eliminou automaticamente um ficheiro infectado? 225

Contacte-nos 226

34. Pedir Ajuda 227

35. Recursos online 229
35.1. Centro de Suporte Bitdefender 229
35.2. Fórum de Suporte Bitdefender 230
35.3. Portal HOTforSecurity 230

36. Informação de Contacto 231
36.1. Endereços Web 231
36.2. Distribuidores locais 231
36.3. Escritórios Bitdefender 232

Glossário 234

INSTALAÇÃO

1. A PREPARAR A INSTALAÇÃO

Antes de instalar o Bitdefender Internet Security 2015, complete estes procedimentos para assegurar uma boa instalação:

- Assegure-se que o computador onde vai instalar o Bitdefender contém os requisitos minimos do sistema. Se o seu computador não contém os requisitos mínimos do sistema, o Bitdefender não será instalado ou, se instalado, não trabalhará corretamente e provocará lentidão e instabilidade no sistema. Para ver a lista completa dos requisitos mínimos do sistema, por favor consulte o "*Requisitos do sistema*" (p. 3).
- Ligue-se ao computador utilizando uma conta de Administrador.
- Remova quaisquer outros softwares semelhantes do seu computador. Executar dois programas de segurança simultaneamente poderá afetar o seu funcionamento e causar grandes problemas no sistema. O Windows Defender será desativado durante a instalação.
- Desativar ou remover qualquer programa de firewall que possa estar em execução no computador. Executar dois programas de firewall simultaneamente poderá afetar o seu funcionamento e causar grandes problemas no sistema. A Firewall do Windows será desativada durante a instalação.
- Recomenda-se que o seu computador esteja ligado à Internet durante a instalação, mesmo quando realiza a instalação a partir de um CD/DVD. Se estiverem disponíveis versões mais recentes dos ficheiros da aplicação incluidos no pacote de instalação, o Bitdefender irá descarregá-las e instalá-las.

2. REQUISITOS DO SISTEMA

Só pode instalar o Bitdefender Internet Security 2015 nos computadores que tenham os seguintes sistemas operativos:

- Windows XP com o Service Pack 3 (32 bits)
- Windows Vista com o Service Pack 2
- Windows 7 com o Service Pack 1
- Windows 8
- Windows 8.1

Antes da instalação, certifique-se de que o seu computador cumpre os requisitos mínimos de hardware e software.

Nota

Para descobrir qual o sistema operativo executado no seu computador e as informações de hardware, siga estes passos:

- No **Windows XP**, **Windows Vista** e **Windows 7**, clique com o botão direito do rato em **Computador** no ambiente de trabalho e, em seguida, selecione **Propriedades** no menu.
- No **Windows 8**, a partir do ecrã Iniciar do Windows, localize Computador (por exemplo, pode começar a digitar "Computador" diretamente no menu Iniciar) e, em seguida, clique com o botão direito do rato no seu ícone. Selecione Propriedades no menu inferior. Procure em Sistema o tipo de sistema.

2.1. Requisitos mínimos do sistema

- 1 GB de espaço disponível no disco rígido (pelo menos 800 MB na unidade do sistema)
- Processador de 1.6 GHz
- 1 GB de memória (RAM) para Windows XP, Windows Vista, Windows 7 e Windows 8

2.2. Requisitos de sistema recomendados

- 2 GB de espaço disponível no disco rígido (pelo menos 800 MB na unidade do sistema)
- Processador Intel Core Duo (2 GHz) ou equivalente
- Memória (RAM):
  - 1 GB para o Windows XP

- 1.5 GB para o Windows Vista, Windows 7 e Windows 8

2.3. Requisitos de Software

Para conseguir usar o Bitdefender e todos os seus recursos, o seu computador deve cumprir os seguintes requisitos de software:

- Internet Explorer 8 ou superior
- Mozilla Firefox 14 ou superior
- Chrome 20 ou superior
- Skype 6.3 ou superior
- Yahoo Messenger 9 ou superior
- Microsoft Outlook 2007 / 2010 / 2013
- Microsoft Outlook Express e Windows Mail (em sistemas de 32 bits)
- Mozilla Thunderbird 14 ou superior
- .NET Framework 3.5 (automaticamente instalado com o Bitdefender se estiver em falta)

3. INSTALAÇÃO DO SEU PRODUTO BITDEFENDER

Pode instalar o Bitdefender a partir do CD de instalação do Bitdefender ou utilizando o ficheiro de instalação descarregado do site web da Bitdefender ou de outros sites autorizados (por exemplo, os sites de parceiros da Bitdefender ou de uma loja online). Pode descarregar o ficheiro de instalação do site da Bitdefender seguindo este endereço: http://www.bitdefender.pt/Downloads/.

Se a sua compra abrange mais do que um computador (por exemplo, adquiriu o Bitdefender Internet Security 2015 para 3 PCs), repita o processo de instalação e registe o seu produto com a chave de licença em cada um dos computadores.

- Para instalar o Bitdefender a partir do disco de instalação, insira o disco na unidade de leitura. Uma janela de boas-vindas aparecerá em alguns momentos. Siga as instruções para iniciar a instalação.

  Nota

  O ecrã de boas-vindas proporciona uma opção para copiar o pacote de instalação a partir do disco de instalação para um dispositivo de armazenamento USB. Isto é útil se precisar de instalar Bitdefender num computador que não possui uma drive de disco (por exemplo, num netbook). Insira a pen USB na drive respetiva e depois clique em **Copiar para a USB**. Depois, vá até ao computador sem a drive de disco, insira a pen USB e faça duplo clique no ficheiro runsetup.exe que se encontra na pasta onde guardou o pacote de instalação.

  Se o ecrã de boas-vindas não aparecer, use o Explorador do Windows para explorar o diretório-raiz do CD e faça duplo clique no ficheiro autorun.exe.

- Para instalar o Bitdefender utilizando um ficheiro de instalação descarregado para o seu computador, localize o ficheiro e faça duplo-clique sobre ele.

A validar a instalação

O Bitdefender irá primeiro verificar o seu sistema para validar a instalação.

Se o seu sistema não apresenta os requisitos mínimos para a instalação Bitdefender, você será informado das áreas que precisam de ser melhoradas antes de poder prosseguir.

Se for detetado um programa antivírus incompatível ou uma versão anterior do Bitdefender, será avisado para o remover do seu sistema. Por favor siga as instruções para remover o software do seu sistema, evitando assim que ocorram problemas mais tarde. Pode necessitar de reiniciar o seu computador para concluir a remoção dos programas antivírus detetados.

O pacote de instalação do Bitdefender Internet Security 2015 é continuamente atualizado. Se está a instalar a partir de um CD/DVD, o Bitdefender pode fazer download das versões mais recentes dos ficheiros durante a instalação. Clique em **Sim** quando solicitado de forma a permitir que o Bitdefender faça download dos ficheiros, assegurando assim que está a instalar a versão mais recente do software.

Nota
Fazer download dos ficheiros de instalação pode demorar muito tempo, especialmente se tiver uma ligação à Internet que seja lenta.

Uma vez que a instalação seja validada, o assistente de instalação aparecerá. Siga os passos para instalar o Bitdefender Internet Security 2015.

Passo 1 - Boas-vindas

A janela de boas-vindas permite-lhe escolher o tipo de instalação que deseja levar a cabo.

Para uma experiência de instalação livre de problemas, basta clicar no botão **Instalar**. O Bitdefender será instalado na localização por defeito com as definições por defeito e você saltará directamente para o Passo 3 do assistente.

Caso queira modificar as definições de instalação, clique em **Personalizar**

Duas tarefas adicionais podem ser levadas a cabo durante este passo:

- Por favor leia o Acordo de Licença de Utilizador antes de prosseguir com a instalação. O Acordo de Licença contém os termos e condições ao abrigo dos quais pode usar o Bitdefender Internet Security 2015.

  Se não concorda com estes termos, feche a janela. O processo de instalação terminará e sairá do mesmo.

- Ativar enviar **Relatórios anónimos de utilização**. Ao ativar esta opção, os relatórios que contêm informação sobre como usa o produto são enviados para os servidores Bitdefender. Esta informação é essencial para melhorar

o produto e pode ajudar-nos a oferecer-lhe uma experiência melhor no futuro. Tenha em atenção que estes relatórios não contêm dados confidenciais, tais como o seu nome, endereço de IP ou outros, e que não serão usados para fins comerciais.

Passo 2 - Personalizar definições da instalação

Nota
Este passo apenas aparece se escolheu personalizar a instalação durante o passo anterior.

Estão disponíveis as seguintes opções:

Caminho da Instalação
Por defeito, Bitdefender Internet Security 2015 será instalado em C:\Ficheiros do Programa\Bitdefender\Bitdefender Internet Security 2015. Se deseja alterar este caminho de instalação, clique em **Alterar** e selecione a pasta na qual pretende que o Bitdefender seja instalado.

Configurar definições de proxy
O Bitdefender Internet Security 2015 requer o acesso à Internet para registo do produto, descarregar atualizações de segurança e de produtos, componentes de deteção na nuvem, etc. Se usar uma ligação por proxy em vez de uma ligação direta à Internet, deve selecionar esta opção e configurar as definições.

As definições podem ser importadas do navegador por defeito ou pode introduzi-las manualmente.

Clique em **Instalar** para confirmar as suas preferências e iniciar a instalação. Caso mude de ideias, clique no botão **Utilizar predefinições** correspondente.

Passo 3 - Instalação em curso

Espere até que a instalação termine. É apresentada informação detalhada sobre a evolução.

As áreas críticas do seu sistema são analisadas, as versões mais recentes dos ficheiros da aplicação são descarregadas e instaladas e os serviços do Bitdefender iniciam-se. Este passo pode demorar alguns minutos.

Passo 4 - Instalação terminada

É apresentado um resumo da instalação. Se tiver sido detetado malware activo e removido durante a instalação, pode ser necessário reiniciar o sistema.

Pode ou fechar a janela ou continuar com a a instalação inicial do seu software ao clicar **Introdução**.

Passo 5 - Registar o seu produto

Nota
Este passo apenas aparece se selecionou Introdução durante o passo anterior.

Para completar o registo do seu produto necessita de inserir a chave de licença. É necessária uma ligação ativa à Internet.

Proceda consoante a sua situação:

- **Eu adquiri o produto**

  Neste caso, registe o produto seguindo os seguintes passos:

  1. Selecione **Adquiri o Bitdefender e quero registar-me agora**.
  2. Insira a chave de licença no campo correspondente.

     Nota
     Pode encontrar a sua chave de licença:
     - na etiqueta do CD/DVD.
     - no certificado de licença.
     - no e-mail da sua compra on-line.

  3. Clique em **Registar Agora**.

- **Não possuo uma licença, mas gostaria de experimentar o produto gratuitamente**

  Neste caso, pode utilizar todos os recursos do produto durante 30 dias. Para iniciar o período experimental, selecione **Não possuo uma chave e pretendo experimentar o produto gratuitamente**.

- Clique **Seguinte**.

Passo 6 - Configurar o funcionamento do produto

Bitdefender pode ser configurado para identificar automaticamente as suas ferramentas de trabalho para melhorar a sua experiência em determinadas situações. Utilize o botão para ligar ou desligar os **Perfis**.

Se trabalha, joga ou vê filmes, ative os **Perfis**. Esta ação irá modificar as definições do produto e do sistema para minimizar o impacto no desempenho do seu sistema. Para mais informação, por favor consulte o *"Perfis"* (p. 18).

Clique **Seguinte**.

Passo 7 - Ative o seu produto

A conta MyBitdefender é necessária para que possa usar as funcionalidades online do seu produto. Para mais informação, por favor consulte o *"Conta MyBitdefender"* (p. 41).

Proceda consoante a sua situação.

Quero criar a conta MyBitdefender

Para criar uma conta MyBitdefender com sucesso, siga os seguintes passos:

1. Clique em **Criar uma nova conta**.

   Uma nova janela irá aparecer.

2. Digite as informações solicitadas nos campos correspondentes. Os dados que nos fornecer serão mantidos confidenciais.

   - **Email** - introduza o seu endereço de email.
   - **Nome de Utilizador** - insira um nome de utilizador para a sua conta.
   - **Palavra-passe** - digite a palavra-passe da sua conta. A palavra-passe deve ter pelo menos 6 caracteres de tamanho.
   - **Confirmar palavra-passe** - volte a introduzir a palavra-passe.

   Nota

   Uma vez a conta criada, poderá utilizar o endereço de e-mail fornecido e a palavra-passe para entrar na sua conta em https://my.bitdefender.com.

3. Clique em **Criar**.

4. Antes de poder usar a sua conta, deve concluir o registo. Verifique o seu email e siga as instruções no email de confirmação enviado pela Bitdefender.

Quero iniciar sessão com a minha conta do Microsoft, Facebook ou Google.

Para iniciar sessão com a sua conta Microsoft, Facebook ou Google, siga os seguintes passos:

1. Selecione o serviço que deseja usar. Seá redireccionado para a página de início de sessão daquele serviço.
2. Siga as instruções fornecidas pelo serviço selecionado para ligar a sua conta ao Bitdefender.

> **Nota**
> O Bitdefender não obtém acesso a qualquer informação confidencial como a palavra-passe da conta que usa para iniciar sessão ou a informação particular dos seus amigos ou contactos.

Já tenho uma conta MyBitdefender

Se iniciou anteriormente a sua sessão numa conta do seu produto, o Bitdefender irá detectá-la e avisá-lo para que insira a palavra-passe para iniciar sessão nessa conta.

Se já possui uma conta ativa, maos o Bitdefender não a deteta, oo você simplesmente deseja iniciar fazer login com uma conta diferente, insira o e-mail e a palavra-passe e clique em **Login à MyBitdefender**.

Adiar para mais tarde

Se deseja deixar esta tarefa para mais tarde, clique em **Perguntar mais tarde**. Lembre-se de que tem de fazer login a uma conta para usar as funcionalidades online do produto.

INTRODUÇÃO

4. OS BÁSICOS

Assim que instalar o Bitdefender Internet Security 2015, o seu computador fica protegido contra todos os tipos de malware (tais como vírus, spyware e cavalos de tróia) e ameaças da Internet (tais como hackers, phishing e spam).

A aplicação utiliza a tecnologia Photon para melhorar a velocidade e o desempenho do processo de análise do antimalware. Funciona através da aprendizagem dos padrões de utilização das suas aplicações de sistema para saber o que e quando analisar, minimizando o impacto no desempenho do sistema.

Pode ligar o Autopilot para disfrutar de uma segurança silenciosa onde não necessita de configurar absolutamente nada. No entanto, poderá querer usufruir das definições do Bitdefender para otimizar e melhorar a sua proteção.

Enquanto trabalha, joga ou vê filmes, Bitdefender pode oferecer-lhe uma experiência de utilizador contínua, adiando as tarefas de manutenção, eliminando as interrupções e ajustando os efeitos visuais do sistema. Pode beneficiar de tudo isto ao ativar e configurar os Perfis.

Bitdefender tomará por si a maioria das decisões relacionadas com segurança e raramente surgirão alertas pop-up. Os pormenores sobre as ações tomadas e informações sobre o funcionament do programa encontram-se disponíveis na janela Eventos. Para mais informação, por favor consulte o "*Eventos*" (p. 15).

De vez em quando, deve abrir o Bitdefender e corrigir as incidências existentes. Poderá ter que configurar componentes específicos do Bitdefender ou levar a cabo ações preventivas para proteger o seu computador e os seus dados.

Se ainda não registou o produto, lembre-se de o fazer até que o período de avaliação termine. Para mais informação, por favor consulte o "*A registar o Bitdefender*" (p. 39).

Para usar as funcionalidades online do Bitdefender Internet Security 2015, certifique-se de entrar no seu computador numa conta MyBitdefender. Para mais informação, por favor consulte o "*Conta MyBitdefender* " (p. 41).

A "Como" (p. 48) secção é onde vai encontrar instruções passo-a-passo sobre como levar a cabo as tarefas mais comuns. Se experimentar

incidências durante o uso do Bitdefender, consulte a "*Resolver incidências comuns*" (p. 190) secção de possíveis soluções para os problemas mais comuns.

4.1. A abrir a janela do Bitdefender

Para aceder à interface principal do Bitdefender Internet Security 2015, siga os passos abaixo:

- No **Windows XP**, **Windows Vista** e **Windows 7**:
  1. Clique em **Iniciar** e vá para **Todos os Programas**.
  2. Clique em **Bitdefender 2015**.
  3. Clique em **Bitdefender Internet Security 2015** ou, mais rápido, clique duas vezes no ícone do Bitdefender no tabuleiro do sistema.
- No **Windows 8**:

  A partir do ecrã Iniciar do Windows, localize Bitdefender Internet Security 2015 (por exemplo, pode começar a digitar "Bitdefender" diretamente no menu Iniciar) e, em seguida, clique no seu ícone. Em alternativa, abra a aplicação do ambiente de trabalho e, em seguida, clique duas vezes no ícone do Bitdefender no tabuleiro do sistema.

Para mais informações sobre a janela e ícone do Bitdefender na barra de notificação, por favor consulte "*Interface Bitdefender*" (p. 24).

4.2. A reparar problemas

O Bitdefender utiliza um sistema de emissão de monitoramento para detectar e informá-lo sobre os problemas que podem afectar a segurança do seu computador e dos seus dados. Por defeito, ele irá acompanhar apenas algumas questões que são consideradas muito importantes. No entanto, pode sempre configurá-lo conforme necessário, escolhendo as questões específicas sobre que deseja ser notificado.

As incidências detetadas incluem definições de proteção importantes que estão desligadas e outras condições que podem representar um risco de segurança. Estão organizadas em duas categorias:

- **Incidências críticas** - impedem que o Bitdefender o proteja contra o malware ou representem um risco de segurança importante.

- **Incidências menores (não críticas)** - podem afetar a sua proteção num futuro próximo.

O ícone Bitdefender na área de notificação indica incidências pendentes alterando a sua cor conforme se indica a seguir:

Incidências críticas estão a afetar a segurança do seu sistema. Eles requerem a sua atenção máxima e devem ser corrigidos o mais rapidamente possível.
Incidências não críticas estão a afetar a segurança do seu sistema. Deve verificar e repará-las quando tiver oportunidade.

Além disso, se mover o cursor do rato sobre o ícone, uma janela pop-up irá confirmar a existência de questões pendentes.

Quando abre a janela do Bitdefender, a área do estado de Segurança, na barra de ferramentas superior, irá indicar a natureza dos problemas que afetam o seu sistema.

4.2.1. Assistente Reparar Todas as Incidências

Para resolver as incidências detetadas siga o assistente **Reparar todas as incidências**.

1. Para abrir o assistente, faça uma das seguintes coisas:
   - Clique com o botão direito do rato no ícone do Bitdefender na área de notificação e selecione **Ver problemas de segurança**.
   - Abra a janela do Bitdefender e clique em qualquer lado dentro da área de estado de Segurança, na barra de ferramentas superior (por exemplo, pode clicar naligação **Reparar todas os problemas**).
2. Pode verificar as incidências que afectam a segurança do seu computador e dos dados. Todas as incidências atuais foram selecionadas para serem reparadas.

   Se não quiser resolver uma incidência específica de imediato, limpe a caixa correspondente. Será notificado para especificar durante quanto tempo pretende adiar a reparação da incidência. Escolha a opção desejada no menu e clique em **OK**. Para parar de monitorizar a categoria de problema respetiva, escolha **Permanentemente**.

   O estado da incidência mudará para **Adiar** e não será tomada qualquer ação para a reparar.

3. Para corrigir todos os problemas selecionados, clique em **Corrigir**. Algumas ocorrências são tratadas imediatamente. Para outras, o assistente ajuda-o a resolvê-las.

A incidência que este assistente o ajuda a tratar pode ser agrupada numa destas categorias:

- **Desativar definições de segurança.** Tais incidências são reparadas imediatamente, ao ativar as respetivas definições de segurança.
- **Ferramentas preventivas de segurança que deve realizar.** Quando reparar a incidência, o assistente ajuda-o a completar com sucesso a tarefa.

4.2.2. Configurar os alertas de estado

O Bitdefender informa-o quando são detetadas incidências no funcionamento dos seguintes componentes do programa:

- Firewall
- Antispam
- Antivírus
- Atualização
- Segurança do Navegador

Pode configurar o sistema de alerta para melhor responder às suas necessidades de segurança escolhendo as incidências específicas sobre as quais pretende receber informações. Siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Clique no ícone na parte superior da janela e selecione **Definições Gerais** do menu suspenso.
3. Na janela **Definições Gerais** selecione a barra **Avançadas**.
4. Clique no link de **Configurar estado dos alertas**.
5. Clique nos botões para ligar ou desligar os alertas de estado de acordo com as suas preferências.

4.3. Eventos

O Bitdefender mantém um registo detalhado dos eventos relacionados com a sua atividade no seu computador. Sempre que algo de relevante para a segurança do seu sistema ou informação acontece, uma nova mensagem

é adicionada aos Eventos do Bitdefender, de forma similar a um novo e-mail que aparece na sua pasta A receber.

Os eventos são uma ferramenta importante na monitorização e gestão da proteção do seu Bitdefender. Por exemplo, pode facilmente verificar se a atualização foi executada com sucesso, se foi encontrado malware no seu computador, se as suas tarefas de backup se executaram sem erros, etc. Adicionalmente, pode tomar outras ações se necessário ou alterar ações tomadas pelo Bitdefender.

Para aceder aos registos dos Eventos, faça o seguinte:

1. Abra a janela de Bitdefender.
2. Clique no ícone na parte superior da janela e selecione **Definições Gerais** do menu suspenso.

As mensagens são agrupadas de acordo com o módulo do Bitdefender cuja atividade se relacione com:

- **Antivírus**
- **Firewall**
- **Deteção de Intrusão**
- **Proteção da Internet**
- **Antispam**
- **Safego**
- **TuneUp**
- **Vulnerabilidade**
- **Atualização**

Sempre que ocorrer um evento, pode ser visto um ponto azul no ícone , na parte superior da janela.

Encontra-se disponível uma lista de eventos para cada categoria. Para obter informações sobre um evento em particular da lista, clique no ícone e selecione **Eventos** do menu suspenso. Os detalhes dos eventos são apresentados na parte inferior da janela. Cada evento surge com a seguinte informação: uma breve descrição, a ação do Bitdefender quando este aconteceu e a data e hora em que ocorreu. Pode ser fornecidas opções para tomar mais ações, caso seja necessário.

Pode filtrar eventos por importância e ordem de acontecimento. Existem três tipos de eventos filtrados por importância, sendo cada tipo indicado com um ícone específico:

■ Eventos de **Informação** indicam operações bem sucedidas.
■ O eventos de **Aviso** indicam incidências não críticas. Deve verificar e repará-las quando tiver oportunidade.
■ Os eventos **críticos** indicam problemas críticos. Deve verificá-los imediatamente.

Para visualizar eventos que ocorreram em determinado período de tempo, selecione o período de tempo pretendido no campo correspondente.

Para o ajudar a gerir facilmente os eventos registados, casa secção da janela de Eventos proporciona opções para eliminar ou marcar como lidos todos os eventos daquela secção.

4.4. Autopilot

Para todos os utilizadores que desejam apenas que a sua solução de segurança os proteja sem os incomodar, o Bitdefender Internet Security 2015 foi concebido com um modo AutoPilot incorporado.

Em Autopilot, o Bitdefender aplica uma configuração de segurança ótima e toma, por si, todas as decisões relacionadas com a segurança. Isto significa que não verá pop-ups nem alertas e não terá de configurar quaisquer definições.

No modo Autopilot, o Bitdefender repara automaticamente incidências críticas, ativa opões e gere tranquilamente:

- Proteção antivírus, proporcionada pela análise no acesso e análise contínua.
- Proteção Firewall.
- Proteção da Internet.
- Atualizações Automáticas.

Para ligar ou desligar o Autopilot, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Clique no botão da barra superior do **Modo Utilizador / Autopilot**. Quando o botão está na posição Modo Utilizador, o Autopilot está desligado.

Enquanto o Autopilot estiver ligado, o ícone Bitdefender na área de notificação mudará para .

Importante
Enquanto o Autopilot estiver ligado, se modificar alguma das definições este será desligado.

Para ver o histórico das ações executadas pelo Bitdefender enquanto o Autopilot estava ligado, abra a janela Eventos.

4.5. Perfis e Modo de Bateria

Algumas atividades do computador, tais como os jogos online ou apresentações de vídeo, requerem uma maior capacidade de resposta, elevado desempenho e nenhuma interrupção do sistema. Quando o seu computador portátil está ligado apenas com a bateria, é melhor que operações desnecessárias, que consomem mais energia, sejam adiadas até que o portátil esteja ligado á corrente.

Para se adaptar a estas situações especiais, o Bitdefender Internet Security 2015 inclui dois modos de funcionamento especial:

- Perfis
- Modo de Bateria

4.5.1. Perfis

Os Perfis do Bitdefender atribuem mais recursos do sistema às aplicações em execução, modificando temporariamente as definições de proteção e ajustando a configuração do sistema. Consequentemente, o impacto do sistema na sua atividade é minimizado.

Para adaptar-se a diferentes atividades, o Bitdefender vem com os seguintes perfis:

Perfil Trabalho
: Otimiza a sua eficiência de trabalho ao identificar e ajustar as definições do produto e do sistema.

Perfil de Filme
: Melhora os efeitos visuais e elimina as interrupções ao ver filmes.

Perfil de jogo
: Melhora os efeitos visuais e elimina as interrupções ao jogar.

A ativar e a desativar perfis

Para ativar ou desativar perfis, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Ferramentas**.
3. Clique no módulo de **Perfis**.
4. Na janela **Perfis**, selecione o separador **Definições de Perfis**.
5. Ative ou desative os perfis clicando no botão correspondente.

Configure o Autopilot para monitorizar os perfis

Para uma experiência de utilizador intuitiva, pode configurar o Autopilot para gerir o seu perfil de trabalho. Neste modo, o Bitdefender detecta automaticamente a sua atividade e realiza e aplica definições de otimização do produto.

Para permitir o Autopilot gerir os perfis, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Ferramentas**.
3. Clique no módulo de **Perfis**.
4. Na janela **Perfis**, selecione o separador **Definições de Perfis**.
5. Clique no botão **Permitir o Autopilot gerir os meus perfis** correspondente.

Caso não queira que o seu Perfil seja gerido automaticamente, deixe a caixa desmarcada e escolha manualmente no canto superior direito da interface do Bitdefender.

Para obter mais informações sobre os Perfis, consulte o"*Perfis*" (p. 183)

4.5.2. Modo de Bateria

O Modo de Bateria foi concebido especialmente para utilizadores de portáteis e tablets. O seu objetivo é minimizar o impacto do sistema e do Bitdefender no consumo de energia quando o nível de bateria estiver abaixo do nível que selecionou.

As definições do produto seguinte são aplicadas quando o Bitdefender opera em Modo de Bateria:

- A Atualização Automática do Bitdefender é adiada.

- As análises agendadas são adiadas.
- A Miniaplicação de Segurança é desligada.

O Bitdefender detecta quando o seu portátil está a funcionar na bateria e dependendo do nível de carga, entra automaticamente em Modo de Bateria. Da mesma forma, o Bitdefender sai automaticamente do Modo de Bateria ao detectar que o portátil já não está a funcionar pela bateria.

Para ativar ou desativar o Modo de Bateria, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Ferramentas**.
3. Clique no módulo de **Perfis**.
4. Na janela **Perfis**, selecione o separador **Modo de Bateria**.
5. Ative ou desative o Modo de Bateria automático clicando no botão correspondente.

   Arraste o cursor correspondente pela escala para definir quando o sistema deve começar a funcionar em Modo de Bateria. Por defeito, o modo é ativado quando o nível da bateria cai abaixo dos 30%.

Nota
O Modo de Bateria é ativado, por defeito, em portáteis e tablets.

A configurar o Modo de Bateria

Para configurar o Modo de Bateria, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Ferramentas**.
3. Clique no módulo de **Perfis**.
4. Na janela **Perfis**, selecione o separador **Modo de Bateria**.
5. Clique em **Configurar**.
6. Escolha os ajustes do sistema que serão aplicados selecionando as seguintes opções:
   - Otimize as definições do produto para o modo Bateria.
   - Adie programas em segundo plano e tarefas de manutenção.
   - Adiar as Atualizações Automáticas do Windows.

- Ajuste as definições do plano de energia para o modo Bateria.
- Desative os dispositivos externos e as portas de rede.

7. Clique em **Guardar** para guardar as alterações e fechar a janela.

4.6. Definições de proteção da palavra-passe de Bitdefender

Se não for a única pessoa a utilizar este computador, recomendamos que proteja as suas configurações do Bitdefender com uma palavra-passe.

Para configurar a proteção de palavra-passe para as definições do Bitdefender, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Clique no ícone na parte superior da janela e selecione **Definições Gerais** do menu suspenso.
3. Na janela **Definições Gerais**, selecione o separador **Definições Gerais**.
4. Ligue a protecção por palavra-passe, clicando no botão.
5. Insira a palavra-passe nos dois campos e depois clique em **OK**. A palavra-passe tem de ter pelo menos 8 caracteres.

Depois de definir uma palavra-passe, se alguém tentar mudar as definições do Bitdefender terá primeiro de fornecer a palavra-passe.

Importante

Não se esqueça da sua palavra-passe e registe-a num local seguro. Se esquecer a palavra-passe, terá de reinstalar o programa ou contactar o apoio do Bitdefender.

Para remover a proteção da palavra-passe, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Clique no ícone na parte superior da janela e selecione **Definições Gerais** do menu suspenso.
3. Na janela **Definições Gerais**, selecione o separador **Definições Gerais**.
4. Desligue a protecção por palavra-passe, clicando no botão. Digite a nova palavra-passe e depois clique em **OK**.

Nota
Para alterar a palavra-passe para o seu produto, clique na hiperligação **Alterar palavra-passe**.

4.7. Relatórios anónimos de utilização

Por defeito, o Bitdefender envia relatórios que contêm informação sobre como o usar nos servidores Bitdefender. Esta informação é essencial para melhorar o produto e pode ajudar-nos a oferecer-lhe uma experiência melhor no futuro. Tenha em atenção que estes relatórios não contêm dados confidenciais, tais como o seu nome, endereço de IP ou outros, e que não serão usados para fins comerciais.

Caso queira parar de enviar Relatórios Anónimos de utilização, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Clique no ícone na parte superior da janela e selecione **Definições Gerais** do menu suspenso.
3. Na janela **Definições Gerais** selecione a barra **Avançadas**.
4. Clique no botão para ligar os Relatórios anónimos de utilização.

4.8. Ofertas especiais e notificações de produto

Quando as ofertas promocionais forem disponibilizadas, o produto Bitdefender está configurado para notificá-lo através de uma janela pop-up. Isto dar-lhe-á a oportunidade de aproveitar os preços vantajosos e manter os dispositivos protegidos por um período mais longo.

Adicionalmente, as notificações do produto poderão aparecer quando o utilizador fizer alterações no produto.

Para ativar ou desativar as ofertas especiais e as notificações do produto, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no ícone na parte superior da janela e selecione **Definições Gerais** do menu suspenso.
3. Na janela **Definições Gerais**, selecione o separador **Definições Gerais**.
4. Ative ou desative as ofertas especiais e as notificações do produto clicando no botão correspondente.

As opções de ofertas especiais e de notificações do produto estão ativadas por defeito.

Nota

Depois de desativar as ofertas especiais e as notificações do produto, o Bitdefender irá continuar a mantê-lo informado sobre as ofertas especiais quando utilizar uma versão de avaliação, quando a sua subscrição expirar ou ao utilizar uma versão do produto expirada.

5. INTERFACE BITDEFENDER

O Bitdefender Internet Security 2015 vai de encontro às necessidades quer dos principiantes quer dos utilizadores mais técnicos. Assim, o interface gráfico do utilizador foi desenhado para servir quer uns quer outros.

Para ver o estado do produto e realizar tarefas essenciais, encontra-se disponível o ícone na área de notificação do sistema do Bitdefender a qualquer momento.

A janela principal permite o acesso a informações importantes do produto, a módulos do program e permite-lhe realizar tarefas comuns. Da janela principal, pode aceder à Área de painéis para configurações detalhadas e tarefas administrativas avançadas, e gerir o comportamento do produto utilizando Autopilot e Perfis.

Se deseja manter uma vigilância constante na informação essencial de segurança e ter um acesso rápido a definições chave, adicione o Dispositivo Segurança ao seu ambiente de trabalho.

5.1. Ícone na área de notificação

Para gerir todo o produto mais rapidamente, pode usar o ícone da Bitdefender que se encontra na barra de tarefas.

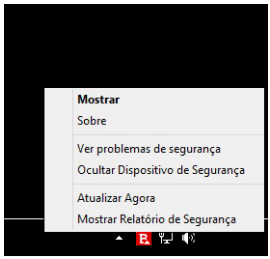
Nota

Se estiver a utilizar o Windows Vista, Windows 7 ou Windows 8, o ícone do Bitdefender poderá não estar sempre visível. Para fazer com que o ícone apareça sempre, faça o seguinte:

1. Clique na seta no canto inferior direito do écran.
2. Clique **Personalizar...** para abrir a janela de ícones da Área de Notificação.
3. Selecione a opção **Mostrar ícones e notificações** para o ícone do **Agente do Bitdefender Agent**.

Se fizer duplo-clique neste ícone, o Bitdefender irá abrir. Também clicando com o botão direito do rato sobre ele aparecerá um menu contextual que lhe permitirá uma administração rápida do Bitdefender.

- **Mostrar** - abre a janela principal do Bitdefender.
- **Acerca** - abre uma janela onde pode ver informação acerca do Bitdefender e onde procurar ajuda caso algo de inesperado lhe apareça.
- **Ver problemas de segurança** - ajuda-o a remover as vulnerabilidades de segurança. Se a opção não está disponível, é porque não há incidências a reparar. Para mais informações, por favor consulte "*A reparar problemas*" (p. 13).



Ícone Tray

- **Ocultar / Mostrar Dispositivo Segurança** - ativa / desativa Dispositivo Segurança.
- **Atualizar agora** - executa uma atualização imediata. Pode seguir o estado da atualização no painel Atualizar da janela principal do Bitdefender.
- **Mostrar Relatório de Segurança** - abre uma janela onde pode visualizar o estado semanal e recomendações para o seu sistema. Pode seguir as recomendações para melhorar a segurança do seu sistema.

O ícone do Bitdefender na área de notificação do sistema, informa quando há incidências a afetar o seu computador ou a forma como o produto funciona, exibindo um símbolo especial, como o que se segue:

Incidências críticas estão a afetar a segurança do seu sistema. Eles requerem a sua atenção máxima e devem ser corrigidos o mais rapidamente possível.
Incidências não críticas estão a afetar a segurança do seu sistema. Deve verificar e repará-las quando tiver oportunidade.
O Autopilot do Bitdefender está ligado.

Se o Bitdefender não estiver a funcionar, o ícone da áea de notificação do sistema fica com uma cor de fundo cinzenta . Isto normalmente acontece quando a licença de chave expira. Também pode ocorrer quando os serviços da Bitdefender não estão a responder ou quando outros erros afectam a actuação normal da Bitdefender.

5.2. Janela Principal

A janela principal do Bitdefender permite-lhe efetuar tarefas comuns, corrigir rapidamente problemas de segurança, ver informações sobre o

funcionamento do produto e configurar as definições do produto. Tudo se encontra a apenas uns cliques de distância.

A janela está organizada em duas áreas principais:

Barra de ferramentas superior
: Aqui é onde pode verificar o estado de segurança do seu computador, configurar o comportamento do Bitdefender em casos especiais e aceder a tarefas importantes.

Área de painéis
: Aqui é onde pode gerir os principais módulos do Bitdefender e executar diferentes tarefas para manter o seu sistema protegido e a funcionar na velocidade ideal.

O ícone , na parte superior da janela, permite-lhe gerir a sua conta e aceder aos recursos online do seu produto a partir do painel da conta. Aqui pode também aceder aos Eventos, os Relatórios de Segurança semanais e a página de Ajuda & Suporte.

Link	Descrição
Número de dias que faltam	O tempo que sobra antes da sua licença atual expirar. Clique no link para abrir a janela onde pode ver mais informação acerca da sua chave de licença ou registar o seu produto com a nova chave de licença.
Comprar	Ajuda-o a adquirir uma chave de licença para o seu produto Bitdefender Internet Security 2015.

5.2.1. Barra de ferramentas superior

A barra de ferramentas superior contém os seguintes elementos:

- A **Área de Estado da Segurança** do lado esquerdo da barra de ferramentas, informa se existem incidências a afetar a segurança do seu computador e ajuda a repará-las.

  A cor da área de estado da segurança muda dependendo das incidências detetadas e são apresentadas diferentes mensagens:

  - **A área está colorida de verde.** Não existem incidências para reparar. O seu computador e os seus dados estão protegidos.

- **A área está colorida de amarelo.** Incidências não críticas estão a afetar a segurança do seu sistema. Deve verificar e repará-las quando tiver oportunidade.
- **A área está colorida de vermelho.** Incidências críticas estão a afetar a segurança do seu sistema. Deve resolver estas incidências imediatamente.

Ao clicar em qualquer lugar na área de estado de segurança, poderá aceder a um assistente que irá ajudar a remover facilmente quaisquer ameaças do seu computador. Para mais informações, por favor consulte "*A reparar problemas*" (p. 13).

- O **Autopilot** permite-lhe executar o Autopilot e desfrutar da segurança de forma completamente silenciosa. Para mais informações, por favor consulte "*Autopilot*" (p. 17).
- Os **Perfis** permitem-lhe trabalhar, jogar ou ver filmes poupando tempo ao configurar o sistema para adiar tarefas de manutenção. Para mais informações, por favor consulte "*Perfis*" (p. 183).

5.2.2. Área de painéis

A área de painéis está dividida em duas partes, uma no lado esquerdo da janela, onde pode aceder e gerir os módulos do Bitdefender, e outra no lado direito da janela, onde pode executar tarefas importantes utilizando os botões de ação.

Os painéis disponíveis nesta área são:

- Proteção
- Privacidade
- Ferramentas
- Botões de ação

Proteção

Neste painel pode configurar o seu nível de segurança, gerir amigos e spammers, ver e editar as definições das ligações à rede e estabelecer quais são as vulnerabilidades do sistema que devem ser corrigidas.

Os módulos que pode gerir no Painel de Proteção são:

Antivírus

A protecção antivirus é a base da sua segurança. O Bitdefender protege-o em tempo real e a pedido contra todos os tipos de malware, tais como vírus, trojans, spyware, adware, etc.

Do módulo Antivírus pode aceder facilmente às seguintes tarefas de análise:

- Análise Rápida
- Análise do Sistema
- Gerir Análises
- Modo de Recuperação

Para mais informações sobre tarefas de análise e como configurar a proteção antivírus, por favor consulte "*Proteção Antivírus*" (p. 87).

Firewall

A firewall protege-o enquanto está ligado às redes e à Internet, através da filtragem de todas as tentativas de ligação.

Para mais informações sobre configuração de firewall, consulte "*Firewall*" (p. 134).

Deteção de Intrusão

A Deteção de Invasão analisa as atividades do sistema e da rede para comportamentos incomuns e possíveis ataques.

Para mais informações sobre como configurar a Deteção de Invasão para proteger a atividade do seu sistema e da sua rede, consulte "*Deteção de Intrusão*" (p. 143).

Proteção da Internet

A proteção da Web ajuda-lhe a manter-se protegido contra ataques de phishing, tentativas de fraude e fugas de dados pessoais enquanto navega na Internet.

Para mais informações sobre como configurar o Bitdefender para proteger a sua atividade Web, consulte "*Proteção da Internet*" (p. 122).

Antispam

O módulo antispam do Bitdefender assegura que a sua Caixa de Entrada permanece livre de emails indesejados através da filtragem do tráfego de email POP3.

Para mais informações sobre a proteção antispam, consulte "*Antispam*" (p. 112).

Vulnerabilidade

O módulo de Vulnerabilidade ajuda-o a manter o sistema operativo e as aplicações que utiliza regularmente atualizados.

Clique em **Análise de Vulnerabilidade** no módulo de Vulnerabilidade para começar a identificar atualizações críticas do Windows, atualizações de aplicações e palavras-passe fracas em contas do Windows.

Para mais informações sobre como configurar a proteção de vulnerabilidade, consulte "*Vulnerabilidade*" (p. 130).

Privacidade

No painel de Privacidade pode encriptar os seus dados privados, proteger as suas transações online, manter a sua experiência de navegação segura e proteger os seus filhos através da visualização e restrição da sua atividade online.

Os módulos que podem ser geridos no Painel de Privacidade são:

Proteção de dados

O módulo de Proteção de Dados impede fugas de dados confidenciais quando estiver online e permite-lhe eliminar ficheiros permanentemente. Clique em **Destruidor de Ficheiros** sob o módulo de proteção de dados para iniciar o assistente que irá permitir-lhe eliminar completamente os ficheiros do seu sistema.

Para mais informações sobre como configurar a Proteção de Dados, consulte "*Proteção de dados*" (p. 126).

Carteira

Carteira é o gestor de palavras-passe que o ajuda a controlar as suas palavras-passe, protege a sua privacidade e proporciona uma experiência de navegação segura.

Do módulo Carteira pode selecionar as seguintes tarefas:

- **Abrir Carteira** - abre a base de dados existente da Carteira.
- **Exportar Carteira** - permite-lhe guardar a base de dados existente numa localização do seu sistema.
- **Criar nova Carteira** - inicia um assistente que lhe permite criar uma nova base de dados da Carteira.

Para obter mais informações sobre a configuração da Carteira, consulte "*Proteção de Carteira para as suas credenciais*" (p. 149).

Controlo Parental

O Controlo Parental do Bitdefender permite monitorizar o que o seu filho está a fazer no computador. Caso haja conteúdo inapropriado, pode decidir restringir o seu acesso à Internet ou às aplicações específicas.

Clique em **Configurar** no módulo do Controlo Parental para iniciar a configuração das contas Windows dos seus filhos e monitorizar a sua atividade onde quer que esteja.

Para mais informações sobre como configurar o Controlo Parental, por favor consulte "*Controlo Parental*" (p. 156).

Safepay

O navegador Bitdefender Safepay™ ajuda a manter a sua atividade bancária online, compras online e qualquer outro tipo de transação online, privada e segura.

Clique em **Abrir Safepay**, no módulo Safepay, para começar a realizar transações online num ambiente seguro.

Para mais informações sobre o Bitdefender Safepay™, consulte "*Segurança Safepay para transações online*" (p. 144).

Ferramentas

No Painel de ferramentas, pode configurar o seu perfil de trabalho, melhorar a velocidade do sistema, fazer backup de ficheiros importantes e ficar protegido enquanto utiliza a sua conta do Facebook.

Os módulos que pode gerir Painel de ferramentas são:

Safego

Bitdefender Safego é a solução de segurança que garante um ambiente online seguro para os utilizadores do Facebook, através da monitorização da sua atividade e dos seus amigos em redes sociais, e alertando contra todas as possíveis publicações maliciosas.

Para mais informação, por favor consulte o "*Proteção Safego para o Facebook*" (p. 168).

TuneUp

Bitdefender Internet Security 2015 oferece não apenas segurança, também ajuda a manter um bom desempenho do seu sistema.

No módulo TuneUp pode aceder a várias ferramentas úteis:

- Otimizador de Um Clique

- Otimizador de Arranque
- Limpa PC
- Desfrag. de Disco
- Limpa Registo
- Restaurador Registo
- Localizador Duplicados

Para mais informações sobre o desempenho das ferramentas de otimização, por favor consulte "*TuneUp*" (p. 174).

Perfis

Os Perfis do Bitdefender ajudam-lhe a ter uma experiência de utilizador simplificada enquanto trabalha, vê um filme ou joga, através da monitorização do produto e das ferramentas de trabalho do sistema. Clique em **Ativar agora** na barra de ferramentas superior da interface do Bitdefender para começar a utilizar este recurso.

O Bitdefender permite-lhe configurar os seguintes perfis:

- Perfil Trabalho
- Perfil de Filme
- Perfil de jogo

Para mais informações sobre como configurar o módulo dos perfis, consulte "*Perfis*" (p. 183).

Botões de ação

A secção dedicada aos botões de ação permite-lhe realizar importantes tarefas relacionadas com a segurança da sua atividade. Sempre que necessitar de fazer uma análise, atualizar o produto, proteger as suas transações online ou otimizar a velocidade do seu sistema, utilize as seguintes opções:

Análise

Execute uma análise rápida para garantir que o seu computador está livre de vírus.

Atualização

Atualize o seu Bitdefender para garantir que tem as assinaturas de malware mais recentes.

Safepay

Abra o Safepay para proteger os seus dados pessoais enquanto efetua transações online.

Otimizar
Liberte espaço no disco, corrija erros de registo e proteja a sua privacidade ao eliminar ficheiros que já não são úteis com um simples clicar no botão.

5.3. Os módulos do Bitdefender

O Bitdefender vem com um número de módulos úteis para ajudá-lo a proteger-se enquanto trabalha, navega na Internet ou efetua pagamentos online, além de melhorar a velocidade do seu sistema e muito mais. Sempre que quiser aceder aos módulos ou começar a configurar o seu produto, clique nos painéis **Proteção**, **Privacidade** e **Ferramentas** na interface do Bitdefender.

A lista seguinte descreve resumidamente cada módulo.

Antivírus
Permite-lhe configurar a sua proteção contra malware, definir exceções de análises e gerir os ficheiros em quarentena.

Antispam
Permite-lhe manter a pasta A Receber livre de SPAM e também configurar as definições do antispam em detalhe.

Proteção da Internet
Permite-lhe saber se as informações das páginas Web que quer visitar são seguras.

Vulnerabilidade
Permite-lhe detectar e corrigir vulnerabilidades do seu sistema.

Proteção de dados
Permite-lhe evitar que ocorram fugas de informação do seu computador e protege a sua privacidade enquanto se encontra online.

Firewall
Permite-lhe configurar as definições gerais da firewall e gerir as regras.

Deteção de Intrusão
Permite-lhe monitorizar e analisar o sistema e as atividades da rede para comportamentos incomuns e possíveis ataques.

Carteira
Permite que aceda às suas credenciais com apenas uma palavra-passe principal.

Perfis
: Permite-lhe definir o seu perfil de trabalho para uma utilização fácil do sistema.

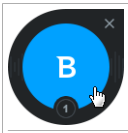
Controlo Parental
: Permite-lhe proteger as suas crianças contra o conteúdo inapropriado, ao usar as suas regras personalizadas de acesso ao computador.

TuneUp
: Permite-lhe monitorizar o desempenho do sue computador e vigiar de perto o consumo de recursos.

5.4. Dispositivo de Segurança

Dispositivo Segurança é a forma rápido e fácil de controlar o Bitdefender Internet Security 2015. Adicionar este dispositivo pequeno e não intrusivo ao seu ambiente de trabalho deixa-o ver informação critica e levar a cabo tarefas chave em qualquer altura:

- abrir a janela principal do Bitdefender.
- monitorizar a atividade de análise em tempo-real.
- monitorizar o estado de segurança do seu sistema e reparar qualquer incidência que exista.
- ver quando uma atualização está em curso.
- ver os avisos e obter acesso aos mais recentes eventos reportados pelo Bitdefender.
- analisar ficheiros ou pastas ao arrastar e largar um ou vários itens sobre o dispositivo.



Dispositivo de Segurança

O estado geral de segurança do seu computador é mostrado **no centro** do dispositivo. O estado é indicado pela cor e forma do ícone que é mostrado nessa área.

Incidências críticas estão a afetar a segurança do seu sistema.

Eles requerem a sua atenção máxima e devem ser corrigidos o mais rapidamente possível. Clique no ícone do estado para começar a reparar as incidências reportadas.

Incidências não críticas estão a afetar a segurança do seu sistema. Deve verificar e repará-las quando tiver oportunidade. Clique no ícone do estado para começar a reparar as incidências reportadas.

O seu sistema está protegido.

Quando uma tarefa de análise a-pedido está em progresso, este ícone animado é apresentado.

Quando são reportadas incidências, clique no ícone de estado para ativar o assistente de Reparação de Incidências.

O lado inferior do dispositivo apresenta o contador de eventos não lidos (o número de eventos importantes comunicados pelo Bitdefender, caso haja algum). Clique no contador de eventos, por exemplo, para um evento não lido, para abrir a janela de Eventos. Para mais informação, por favor consulte o "*Eventos*" (p. 15).

5.4.1. Analisar ficheiros e pastas

Pode usar o Dispositivo de Segurança para analisar rapidamente ficheiros e pastas. Arraste qualquer ficheiro ou pasta que deseje analisar e largue-o sobre o **Dispositivo Segurança**.

O Assistente de Análise Antivírus irá surgir e guiá-lo através do processo de análise. As opções de análise estão pré-configuradas para obter os melhores resultados de deteção e não podem ser alterados Se forem detectados ficheiros infectados, o Bitdefender irá tentar desinfectá-los (remover o código de malware). Se a desinfecção falha, o assistente de análise antivírus irá permitir-lhe definir outras acções a serem levadas a cabo sobre os ficheiros infectados.

5.4.2. Ocultar / mostrar Dispositivo de Segurança

Quando não desejar mais ver o dispositivo, clique em .

Para restaurar o Widget de Segurança, utilize um dos seguintes métodos:

- Do tabuleiro do sistema:
  1. Clique com o botão direito do rato no ícone do Bitdefender no ícone do tabuleiro do sistema.
  2. Clique em **Mostrar Dispositivo Segurança** no menu contextual que aparece.
- A partir da interface do Bitdefender:
  1. Abra a janela de Bitdefender.
  2. Clique no ícone na parte superior da janela e selecione **Definições Gerais** do menu suspenso.
  3. Na janela **Definições Gerais**, selecione o separador **Definições Gerais**.
  4. Ligar **Exibir Widget de Segurança** ao clicar no botão correspondente.

5.5. Relatório de Segurança

O Relatório de Segurança fornece um estado semanal para o seu produto e diversas dicas para melhorar a proteção do sistema. Estas dicas são importantes para gerir a proteção geral e poderá facilmente identificar as ações que pode tomar para o seu sistema.

O relatório é gerado uma vez por semana e resume informações relevantes sobre as atividades do produto para que possa facilmente compreender o que ocorreu durante este período.

As informações oferecida pelo Relatório de Segurança dividem-se em duas categorias:

- Área de **Proteção** - veja as informações relacionadas com a proteção do seu sistema.
  - **Ficheiros analisados**

    Permite-lhe visualizar os ficheiros analisados pelo Bitdefender durante a semana. Pode ver detalhes como o número de ficheiros analisados e o número de ficheiros limpos pelo Bitdefender.

    Para obter mais informações sobre a proteção antivírus, consulte "*Proteção Antivírus*" (p. 87).
  - **Páginas Web analisadas**

Permite-lhe verificar o número de páginas Web analisadas e bloqueadas pelo Bitdefender. Para o proteger da divulgação de informações pessoais durante a navegação, o Bitdefender protege o seu tráfego na Internet.

Para mais informações sobre a Proteção da Internet, consulte "*Proteção da Internet*" (p. 122).

- **Vulnerabilidades**

  Permite identificar e corrigir facilmente as vulnerabilidades do sistema, para tornar o computador mais seguro contra malware e hackers.

  Para obter mais informações sobre a análise de vulnerabilidade, consulte "*Vulnerabilidade*" (p. 130).

- **Linha Cronológica de Eventos**

  Permite que tenha uma imagem geral de todos os processos de análise e problemas corrigidos pelo Bitdefender durante a semana. Os eventos são separados por dias.

  Para mais informações sobre um registo detalhado de eventos relativos à atividade no seu computador, consulte Eventos.

- Área de **Otimização** - veja informações relacionadas com o espaço libertado, aplicações otimizadas e quanta bateria do computador economizou utilizando o Modo de Bateria.

  - **Espaço libertado**

    Permite-lhe ver quanto espaço foi libertado durante o processo de otimização do sistema. O Bitdefender utiliza o TuneUp para ajudar a melhorar a velocidade do sistema.

    Para mais informações sobre o TuneUp, consulte "*TuneUp*" (p. 174).

  - **Bateria economizada**

    Permite-lhe ver quanta bateria economizou enquanto o sistema funcionou em Modo de Bateria.

    Para mais informações sobre o Modo de Bateria, consulte "*Modo de Bateria*" (p. 19).

  - **Aplicações otimizadas**

    Permite-lhe ver o número de aplicações utilizadas nos Perfis.

    Para mais informações sobre Perfis, consulte "*Perfis*" (p. 183).

5.5.1. A verificar o Relatório de Segurança

O Relatório de Segurança utiliza um sistema de rastreio de problemas para detectar e o informar sobre os problemas que podem afetar a segurança do seu computador e dados. As incidências detetadas incluem definições de proteção importantes que estão desligadas e outras condições que podem representar um risco de segurança. Ao utilizar o relatório, pode configurar componentes específicos do Bitdefender ou tomar ações preventivas para proteger o seu computador e dados privados.

Para verificar o Relatório de Segurança, siga estes passos:

1. Aceder ao relatório:
   - Abra a janela do Bitdefender, clique no ícone na parte superior da janela e, em seguida, selecione **Relatório de Segurança** do menu suspenso.
   - Clique com o botão direito do rato no ícone do Bitdefender no tabuleiro do sistema e selecione **Mostrar relatório de segurança**.
   - Após a conclusão de um relatório receberá uma notificação pop-up. Clique em **Mostrar** para aceder ao relatório de segurança.

     Abrir-se-á uma página Web no navegador Web onde pode visualizar o relatório gerado.
2. Observe a parte superior da janela para visualizar o estado geral de segurança.
3. Verifique as nossas recomendações na parte inferior da página.

A cor da área de estado da segurança muda dependendo das incidências detetadas e são apresentadas diferentes mensagens:

- **A área está verde.** Não existem problemas a corrigir. O seu computador e os seus dados estão protegidos.
- **A área está amarela.** A segurança do seu sistema está a ser afetada por problemas não críticos. Deve verificar e repará-las quando tiver oportunidade.
- **A área está vermelha.** A segurança do seu sistema está a ser afetada por problemas críticos. Deve resolver estas incidências imediatamente.

5.5.2. Ativar ou desativar a notificação do Relatório de Segurança

Para ligar ou desligar a notificação do Relatório de Segurança, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no ícone na parte superior da janela e selecione **Definições Gerais** do menu suspenso.
3. Na janela **Definições Gerais**, selecione o separador **Definições Gerais**.
4. Clique no botão correspondente para ativar ou desativar a notificação do Relatório de Segurança.

   A notificação do Relatório de Segurança está ativada por defeito.

6. A REGISTAR O BITDEFENDER

De forma a estar protegido pelo Bitdefender, deve de registar o seu produto com a chave de licença. A chave de licença especifica durante quanto tempo pode usar o produto. Assim que a chave de licença expira, o Bitdefender pára de executar as suas funções e de proteger o seu computador.

Deve de adquirir uma chave de licença ou renovar a sua licença uns dias antes da atual licença expirar. Para mais informação, por favor consulte o "*Adquirir ou renovar chaves de licença*" (p. 40). Se estiver a utilizar a versão teste do Bitdefender, deve registar o produto com uma chave de licença caso pretenda continuar a utilizá-lo após o término do período de teste.

6.1. Inserir a sua chave de licença

Se selecionou avaliar o produto durante a instalação, poderá utilizá-lo por um período de avaliação de 30 dias. Para continuar a utilizar o Bitdefender quando o período de teste expirar, deve registar o produto com uma chave de licença.

Um link que indica o número de dias que sobram à sua licença aparece no fundo da janela do Bitdefender. Clique nesse link para abrir a janela de registo.

Pode ver o estado do registo do Bitdefender, a atual chave de licença e quantos dias faltam para a licença expirar.

Para registar Bitdefender Internet Security 2015:

1. Insira a chave de licença no campo correspondente.

   Nota
   Pode encontrar a sua chave de licença:
   - Na bolsa do CD.
   - no certificado de licença.
   - no e-mail da sua compra on-line.

   Se não tiver uma chave de licença do Bitdefender, clique na hiperligação fornecida na janela para abrir a página web onde poderá adquirir uma.

2. Clique em **Registar Agora**.

Mesmo depois de comprar uma chave de licença, até que o registo interno do produto com essa chave esteja completo, o Bitdefender Internet Security 2015 continuará a funcionar como uma versão demo.

6.2. Adquirir ou renovar chaves de licença

Se o período de testes vai terminar em breve, deve de adquirir uma chave de licença e registar o seu produto. De igual modo, se a sua atual chave de licença vai expirar brevemente, deve renová-la.

O Bitdefender alerta quando se aproxima a data de expiração da sua actual licença. Siga as instruções no alerta para adquirir uma nova licença.

Pode visitar uma página web a partir da qual pode adquirir em qualquer momnto uma chave de licença, seguindo os seguintes passos:

1. Abra a janela de Bitdefender.
2. Clique no link que indica os dias que sobram para a sua licença, localizado no fundo da janela do Bitdefender, para abrir a janela de registo do produto.
3. Clique em **Não tem uma chave de licença? Compre uma agora!**
4. Abre-se uma página web no seu navegador onde pode adquirir a chave de licença do Bitdefender.

7. CONTA MYBITDEFENDER

As funcionalidades online do seu produto e os serviços adicionais do Bitdefender só estão disponíveis através da MyBitdefender. Deve de entrar na MyBitdefender fazendo login à sua conta através do Bitdefender Internet Security 2015 de forma a poder fazer o seguinte:

- Recuperar a sua chave de licença, caso alguma vez a perca.
- Configurar as definições do Controlo Parental para as contas Windows das suas crianças e monitorizar a sua atividade onde quer que eles estejam.
- Obtenha proteção para a sua conta Facebook com Safego.
- Gerir o Bitdefender Internet Security 2015 remotamente.

Multiplas soluções de segurança do Bitdefender para PCs como também para outras plataformas integram-se com a MyBitdefender. Pode gerir a segurança de todos os dispositivos ligados à sua conta a partir de um painel de controlo centralizado.

A sua conta MyBitdefender pode ser acedida a partir de qualquer dispositivo ligado à Internet em https://my.bitdefender.com.

Pode também aceder e gerir a sua conta diretamente do seu produto:

1. Abra a janela de Bitdefender.
2. Clique no ícone na parte superior da janela e selecione **MyBitdefender** no menu suspenso.

7.1. Ligar o seu computador à MyBitdefender

Para ligar o seu computador à conta MyBitdefender, deve de fazer login à mesma a partir do Bitdefender Internet Security 2015. Até que ligue o seu computador à MyBitdefender, será avisado para fazer login à MyBitdefender cada vez que quiser usar uma funcionalidade que requeira uma conta.

Para abrir a janela MyBitdefender a partir da qual pode criar ou fazer login a uma conta, faça o seguinte:

1. Abra a janela de Bitdefender.
2. Clique no ícone na parte superior da janela e selecione **Informações da Conta** no menu suspenso.

Se já fez iniciou sessão numa conta, a conta à qual está ligado é apresentada. Clique em **Iniciar sessão com outra conta** para alterar a conta ligada ao computador.

Se já fez login a uma conta, a conta à qual está ligado é apresentada. Clique em **Ir para MyBitdefender** para ir para o seu painel. Para alterar a conta associada ao computador, clique em **Iniciar sessão com outra conta**.

Se ainda não fez login a uma conta, proceda de acordo com a sua situação.

Quero criar a conta MyBitdefender

Para criar uma conta MyBitdefender com sucesso, siga os seguintes passos:

1. Clique em **Criar uma nova conta**.

   Uma nova janela irá aparecer.

2. Digite as informações solicitadas nos campos correspondentes. Os dados que nos fornecer serão mantidos confidenciais.

   - **Email** - insira o seu endereço de email.
   - **Nome de Utilizador** - insira um nome de utilizador para a sua conta.
   - **Palavra-passe** - digite a palavra-passe da sua conta. A palavra-passe deve ter pelo menos 6 caracteres de tamanho.
   - **Confirmar palavra-passe** - volte a introduzir a palavra-passe.

3. Clique em **Criar**.
4. Antes de poder usar a sua conta, deve concluir o registo. Verifique o seu email e siga as instruções no email de confirmação enviado pela Bitdefender.

Quero iniciar sessão com a minha conta do Microsoft, Facebook ou Google.

Para iniciar sessão com a sua conta Microsoft, Facebook ou Google, siga os seguintes passos:

1. Clique no ícone do serviço que deseja usar para iniciar sessão. Seá redireccionado para a página de início de sessão daquele serviço.
2. Siga as instruções fornecidas pelo serviço selecionado para ligar a sua conta ao Bitdefender.

Nota
O Bitdefender não obtém acesso a qualquer informação confidencial como a palavra-passe da conta que usa para iniciar sessão ou a informação particular dos seus amigos ou contactos.

Já tenho uma conta MyBitdefender

Se já tem uma conta mas ainda não fez login à mesma, faça o seguinte para entrar na conta:

1. Digite o endereço de e-mail e a palavra-passe da sua conta nos campos correspondentes.

   Nota
   Se não se lembra da sua palavra-passe, clique em **Esqueceu-se da sua palavra-passe?** e siga as instruções para a recuperar.

2. Clique em **Login à MyBitdefender**.

Uma vez que o computador esteja ligado a uma conta, pode usar o e-mail e palavra-passe que definiu para fazer login à https://my.bitdefender.com.

Também pode aceder a sua conta diretamente do Bitdefender Internet Security 2015 clicando no ícone na parte superior da janela e selecionando **MyBitdefender** no menu suspenso.

8. MANTENHA O SEU BITDEFENDER ATUALIZADO.

Todos os dias são encontrados e identificados novos vírus. Esta é a razão pela qual é muito importante manter o Bitdefender actualizado com as últimas assinaturas de malware.

Se está ligado à Internet através de banda larga ou ADSL, o Bitdefender executa esta operação sozinho. Por defeito, quando liga o computador verifica se há actualizações e depois disso fá-lo a cada **hora** . Se forem detetadas atualizações, serão automaticamente descarregadas e instaladas no seu computador.

O processo de actualização é executado "on the fly", o que significa que os ficheiros são substituidos progressivamente. Desta forma, o processo de actualização não afectará o funcionamento do produto e, ao mesmo tempo, exclui qualquer possibilidade de vulnerabilidade.

Importante

Para estar protegido contra as mais recentes ameaças mantenha a Atualização Automática ativada.

Nalgumas situações particulares, a sua intervenção é necessária para manter a proteção do Bitdefender atualizada:

- Se o seu computador se ligar a Internet através de um servidor proxy, você deve configurar as definições do proxy conforme escrito em "*Como posso configurar Bitdefender para usar um proxy de ligação à Internet?*" (p. 80).
- Se não possui uma ligação à Internet, pode atualizar Bitdefender manualmente conforme descrito em "*O Meu Computador não está ligado à Internet. Como posso actualizar o Bitdefender?*" (p. 201). O ficheiro de atualização manual é publicado uma vez por semana.
- Podem ocorrer erros ao descarregar atualizações com uma ligação lenta à Internet. Para saber como ultrapassar tais erros, consulte "*Como atualizar o Bitdefender numa ligação à Internet lenta*" (p. 201).
- Se está ligado à Internet através de uma ligação dial-up, então é uma boa ideia adquirir o hábito de atualizar o Bitdefender a seu pedido. Para mais informação, por favor consulte o "*A efetuar uma atualização*" (p. 45).

8.1. Verifique se o Bitdefender está atualizado

Para verificar se a proteção de Bitdefender está atualizada, siga estes passos:

1. Abra a janela de Bitdefender.
2. Na **Área do Estado de Segurança**, no lado esquerdo da barra de ferramentas, procure a hora da última atualização.

Para informações mais detalhadas acerca das mais recentes atualizações, verifique os eventos de atualização:

1. Na janela principal, clique no ícone na parte superior da janela e selecione **Eventos** no menu suspenso.
2. Na janela **Eventos**, selecione **Atualizar** no menu suspenso correspondente.

Você pode saber quando foram iniciadas as atualizações e obter informações sobre as mesmas (se foram bem sucedidas ou não, se é necessário reiniciar para concluir a instalação). Se necessário, reinicie o sistema quando lhe convier.

8.2. A efetuar uma atualização

Para realizar atualizações, é necessária uma ligação à Internet.

Para iniciar uma atualização, faça o seguinte:

- Abra a janela do Bitdefender e clique no botão **Atualizar** à direita da janela.
- Clique com o botão direito no ícone do Bitdefender na barra de sistema e selecione **Atualizar Agora**.

O módulo Atualização irá ligar-se ao servidor de atualização de Bitdefender e verificará se existem atualizações. Se uma atualização é detetada, poderá ser notificado para confirmar a atualização ou a mesma é realizada automaticamente, dependendo das definições de atualização.

Importante
Poderá ser necessário reiniciar o computador quando a actualização tiver terminado. Recomendamos que o faça assim que seja possível.

8.3. Ligar ou desligar a atualização automática

Para ativar ou desativar a análise automática, siga estes passos:

1. Abra a janela de Bitdefender.

2. Clique no ícone na parte superior da janela e selecione **Definições Gerais** do menu suspenso.
3. Na janela de **Definições Gerais**, selecione o separador **Atualizar**.
4. Clique no botão para ativar ou desativar a atualização automática.
5. Uma janela de aviso irá aparecer. Tem de confirmar a sua escolha selecionando no menu durante quanto tempo pretende desativar a atualização automática. Pode desactivar a actualização automática durante 5, 15 ou 30 minutos, por uma hora, permanentemente ou até que o sistema reinicie.

Atenção
Esta é uma incidência de segurança critica. Recomendamos que desative a atualização automática o menos tempo possível. Se o Bitdefender não for atualizado regularmente, não será capaz de o proteger contra as ameaças mais recentes.

8.4. Ajuste das configurações da atualização

As atualizações podem ser executadas através da rede local, da Internet, diretamente ou através de um servidor proxy. Por defeito, o Bitdefender verificará as atualizações a cada hora, via Internet, e instalará as que estejam disponíveis sem o avisar.

As definições de atualização por defeito são adequadas à maioria dos utilizadores e normalmente não tem de as alterar.

Para ajustar as definições de atualização, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no ícone na parte superior da janela e selecione **Definições Gerais** do menu suspenso.
3. Na janela **Definições Gerais**, selecione o separador **Atualizar** e ajuste as definições de acordo com suas preferências.

Atualizar localização

Bitdefender está configurado para ser atualizado a partir dos servidores de atualização de Bitdefender na Internet. A localização de atualização é um endereço genérico da Internet que é automaticamente redireccionado para o servidor de atualização da Bitdefender mais próximo da sua região.

Não altere a localização da atualização exceto se tiver sido aconselhado por um representante da Bitdefender ou pelo administrador da sua rede (se estiver ligado a uma rede no escritório).

Pode voltar à localização de atualização genérica da Internet clicando em **Predefinição**.

Regras de atualização

Pode escolher entre três formas para descarregar e instalar atualizações:

- **Atualização silenciosa** - O Bitdefender faz automaticamente o download e a implementação da atualização.
- **Avisar antes de descarregar** - sempre que uma atualização está disponível, será consultado antes do download ser feito.
- **Avisar antes de instalar** - cada vez que uma atualização for descarregada, será consultado antes da instalação ser feita.

Algumas atualizações exigem o reinício para concluir a instalação. Por defeito, se for necessário reiniciar após uma actualização, o Bitdefender continuará a trabalhar com os ficheiros antigos até que o utilizador reinicie voluntariamente o computador. Isto serve para evitar que o processo de actualização de Bitdefender interfira com o trabalho do utilizador.

Se quiser ser avisado quando uma atualização requere um reinício, desligue a opção **Adiar reiniciar** clicando no botão correspondente.

COMO

9. INSTALAÇÃO

9.1. Como instalo o Bitdefender num segundo computador?

Se adquiriu uma chave de licença para mais de um computador, pode usar a mesma chave de licença para registar um segundo PC.

Para instalar o Bitdefender corretamente num segundo computador, faça o seguinte:

1. Instale o Bitdefender a partir do CD/ DVD ou usando o instalador fornecido através do email da compra online e siga os mesmos passos de instalação.

   No início da instalação ser-lhe-á solicitada a transferência dos ficheiros de instalação mais recentes disponíveis.

2. Quando a janela de registo aparece, insira a chave de licença e clique **Registar Agora**.

3. No próximo passo, tem a opção de fazer login à sua conta MyBitdefender ou criar uma nova conta MyBitdefender.

   Pode também escolher criar uma conta MyBitdefender mais tarde.

4. Aguarde até que o processo de instalação esteja concluído e feche a janela.

9.2. Quando é que devo reinstalar o Bitdefender?

Nalgumas situações poderá ter de reinstalar o seu produto Bitdefender.

As situações típicas em que deve reinstalar Bitdefender são as seguintes:

- você reinstalou o sistema operativo.
- adquiriu um computador novo.
- deseja alterar a língua da interface do Bitdefender.

Para reinstalar o Bitdefender pode usar o disco de instalação que adquiriu ou descarregue uma nova versão do site web Bitdefender.

Durante a instalação, ser-lhe-á pedido que registe o produto com a sua chave de licença.

Se perder a sua chave de licença, pode iniciar sessão na https://my.bitdefender.com e recuperá-la. Digite o endereço de e-mail e a palavra-passe da sua conta nos campos correspondentes.

Para obter mais informações sobre o processo de instalação do Bitdefender, consulte "*Instalação do seu produto Bitdefender*" (p. 5).

9.3. Onde posso transferir o meu produto Bitdefender?

Pode transferir o seu produto Bitdefender a partir dos nossos sites Web autorizados (por exemplo, o site Web de um parceiro Bitdefender ou uma loja online) ou a partir do nosso site Web no seguinte endereço: http://www.bitdefender.pt/Downloads/.

Nota
Antes de executar o kit, é recomendada a remoção de qualquer solução antivírus instalada no seu sistema. Quando utiliza mais do que uma solução de segurança no mesmo computador, o sistema torna-se instável.

Para instalar o Bitdefender, siga estes passos:

1. Clique duas vezes no instalador transferido e siga os passos de instalação.
2. Quando a janela de registo aparece, insira a chave de licença e clique **Registar Agora**.
3. No próximo passo, tem a opção de fazer login à sua conta MyBitdefender ou criar uma nova conta MyBitdefender.

   Pode também escolher criar uma conta MyBitdefender mais tarde.
4. Aguarde até que o processo de instalação esteja concluído e feche a janela.

9.4. Como posso mudar de um produto Bitdefender para outro?

Pode facilmente mudar de um produto Bitdefender para outro.

Os três produtos Bitdefender que pode instalar no seu sistema são:

- Bitdefender Antivirus Plus 2015
- Bitdefender Internet Security 2015
- Bitdefender Total Security 2015

Caso não possua uma chave de licença para o produto que pretende utilizar, siga estes passos:

1. Abra a janela de Bitdefender.
2. Para aceder à janela de registo do produto, clique na hiperligação que indica o número de dias restantes da sua licença, localizada na parte inferior da janela do Bitdefender.
3. Clique em **Não tem uma chave de licença? Compre uma agora!**
4. Abre-se uma página web no seu navegador onde pode adquirir a chave de licença do Bitdefender.

Após comprar a chave de licença para o produto Bitdefender que pretende utilizar, siga estes passos:

1. Abra a janela de Bitdefender.
2. Um link que indica o número de dias que sobram à sua licença aparece no fundo da janela do Bitdefender.

   Clique nesse link para abrir a janela de registo.
3. Introduza a nova chave de licença e clique em **Registrar agora**.
4. Será informado de que a chave de licença é para um produto Bitdefender diferente.

   Clique no respetivo link e siga o procedimento para levar a cabo a instalação.

9.5. Como utilizo a minha chave de licença do Bitdefender após a atualização do Windows?

Esta situação ocorre quando atualiza o sistema operativo e pretende continuar a utilizar a chave de licença do Bitdefender.

Se estiver a utilizar uma versão anterior do Bitdefender, pode atualizar, gratuitamente para a versão mais recente do Bitdefender, da seguinte forma:

- Da versão anterior do Bitdefender Antivirus para a versão mais recente doBitdefender Antivirus.
- Da versão anterior do Bitdefender Internet Security para a versão mais recente do Bitdefender Internet Security.

- Da versão anterior do Bitdefender Total Security para a versão mais recente do Bitdefender Total Security.

Existem 2 casos que podem surgir:

- Atualizou o sistema operativo utilizando o Windows Update e constata que o Bitdefender já não funciona.

  Neste caso, será necessário reinstalar o produto utilizando a versão mais recente disponível.

  Para resolver esta situação, siga estes passos:

  1. Remova o Bitdefender seguindo estes passos:
     - No **Windows XP**:
       a. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Adicionar/Remover Programas**.
       b. Encontre o **Bitdefender Internet Security 2015** e selecione **Remover**.
       c. Clique em **Remover** na janela que aparece e depois selecione **Eu quero reinstalá-lo**.
       d. Aguarde que o processo de desinstalação conclua e, em seguida, reinicie o sistema.
     - No **Windows Vista** e **Windows 7**:
       a. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.
       b. Encontre o **Bitdefender Internet Security 2015** e selecione **Desinstalar**.
       c. Clique em **Remover** na janela que aparece e depois selecione **Eu quero reinstalá-lo**.
       d. Aguarde que o processo de desinstalação conclua e, em seguida, reinicie o sistema.
     - No **Windows 8**:
       a. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
       b. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.

c. Encontre o **Bitdefender Internet Security 2015** e selecione **Desinstalar**.

d. Clique em **Remover** na janela que aparece e depois selecione **Eu quero reinstalá-lo**.

e. Aguarde que o processo de desinstalação conclua e, em seguida, reinicie o sistema.

2. Transfira o arquivo de instalação ao escolher o produto para o qual possui uma chave de licença válida.

   Pode descarregar o ficheiro de instalação do site da Bitdefender seguindo este endereço: http://www.bitdefender.pt/Downloads/.

3. Clique duas vezes no instalador para iniciar o processo de instalação.

4. Quando a janela de registo aparece, insira a chave de licença e clique **Registar Agora**.

5. No próximo passo, pode optar por iniciar sessão na sua conta **MyBitdefender** ou criar uma nova conta **MyBitdefender**.

   Também pode optar por criar uam conta **MyBitdefender** mais tarde.

   Aguarde até que o processo de instalação esteja concluído e feche a janela.

- Alterou o seu sistema e pretende continuar a utilizar a proteção Bitdefender.

  Portanto, será necessário reinstalar o produto utilizando a versão mais recente.

  Para resolver esta situação, siga estes passos:

  1. Transfira o arquivo de instalação ao escolher o produto para o qual possui uma chave de licença válida.

     Pode descarregar o ficheiro de instalação do site da Bitdefender seguindo este endereço: http://www.bitdefender.pt/Downloads/.

  2. Clique duas vezes no instalador para iniciar o processo de instalação.

  3. Quando a janela de registo aparece, insira a chave de licença e clique **Registar Agora**.

  4. No próximo passo, pode optar por iniciar sessão na sua conta **MyBitdefender** ou criar uma nova conta **MyBitdefender**.

Também pode optar por criar uam conta **MyBitdefender** mais tarde.

Aguarde até que o processo de instalação esteja concluído e feche a janela.

Para obter mais informações sobre o processo de instalação do Bitdefender, consulte "*Instalação do seu produto Bitdefender*" (p. 5).

9.6. Como reparo o Bitdefender?

Caso pretenda reparar o Bitdefender Internet Security 2015 a partir do menu Iniciar do Windows, siga estes passos:

- No **Windows XP**, **Windows Vista** e **Windows 7**:
  1. Clique em **Iniciar** e vá para **Todos os Programas**.
  2. Encontre o **Bitdefender Internet Security 2015** e selecione **Desinstalar**.
  3. Clique em **Reparar** na janela que aparece.

     Isto irá demorar vários minutos.
  4. Precisará de reiniciar o computador para concluir o processo
- No **Windows 8**:
  1. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
  2. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.
  3. Encontre o **Bitdefender Internet Security 2015** e selecione **Desinstalar**.
  4. Clique em **Reparar** na janela que aparece.

     Isto irá demorar vários minutos.
  5. Precisará de reiniciar o computador para concluir o processo

10. REGISTO

10.1. Que produto Bitdefender estou a usar?

Para saber que programa Bitdefender instalou, siga estes passos:

1. Abra a janela de Bitdefender.
2. No cimo da janela deverá ver um dos seguintes:
   - Bitdefender Antivirus Plus 2015
   - Bitdefender Internet Security 2015
   - Bitdefender Total Security 2015

10.2. Como posso registar uma versão teste?

Se instalou uma versão teste, só a poderá usar durante um período de tempo limitado. Para continuar a usar o Bitdefender quando o período de avaliação expirar, deve de registar o seu produto com uma chave de licença.

Para registar o Bitdefender, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Um link que indica o número de dias que sobram à sua licença aparece no fundo da janela do Bitdefender.

   Clique nesse link para abrir a janela de registo.
3. Introduza a chave de registo e clique em **Registar Agora**.

   Se não tiver uma chave de licença, clique na ligação fornecida na janela para visitar a página web onde poderá adquirir uma.
4. Aguarde até que o processo de registo esteja concluído e feche a janela.

10.3. Quando é que a proteção do Bitdefender expira?

Para saber quantos dias restam para a chave da sua licença expirar, siga estes passos:

1. Abra a janela de Bitdefender.
2. Um link que indica o número de dias que sobram à sua licença aparece no fundo da janela do Bitdefender.

3. Para mais informação, clique no link para abrir a janela de registo.
4. Na janela **Registar o Produto**, pode:
   - Ver a chave de licença atual
   - Registar com outra chave de licença
   - Comprar uma chave de licença

10.4. Como posso renovar a proteção do meu Bitdefender?

Quando a proteção do seu Bitdefender estiver quase a expirar, deve renovar a sua chave de licença.

- Siga os seguintes passos para visitar um síio web onde pode renovar a sua chave de licença do Bitdefender:
  1. Abra a janela de Bitdefender.
  2. Um link que indica o número de dias que sobram à sua licença aparece no fundo da janela do Bitdefender. Clique nesse link para abrir a janela de registo.
  3. Clique em **Não tem uma chave de licença? Compre uma agora!**
  4. Abre-se uma página web no seu navegador onde pode adquirir a chave de licença do Bitdefender.

  > **Nota**
  > Como alternativa, pode contactar o revendedor onde aquiriu o produto Bitdefender.

- Siga estes passos para registar o seu Bitdefender com a nova chave de licença:
  1. Abra a janela de Bitdefender.
  2. Um link que indica o número de dias que sobram à sua licença aparece no fundo da janela do Bitdefender. Clique nesse link para abrir a janela de registo.
  3. Introduza a chave de registo e clique em **Registar Agora**.
  4. Aguarde até que o processo de registo esteja concluído e feche a janela.

Para mais informações, poderá contactar a Bitdefender para suporte, como descrito na seccção “*Pedir Ajuda*” (p. 227).

11. MYBITDEFENDER

11.1. Como inicio sessão na MyBitdefender utilizando outra conta online?

Criou uma nova conta MyBitdefender e pretende utilizá-la de agora em diante.

Para utilizar outra conta com sucesso, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no ícone na parte superior da janela e selecione **Informações da Conta** no menu suspenso.

   Se já fez iniciou sessão numa conta, a conta à qual está ligado é apresentada. Clique em **Iniciar sessão com outra conta** para alterar a conta ligada ao computador.

   Uma nova janela irá aparecer.
3. Digite o endereço de e-mail e a palavra-passe da sua conta nos campos correspondentes.
4. Clique em **Login à MyBitdefender**

11.2. Como altero o endereço de e-mail utilizado para a conta MyBitdefender?

Criou uma conta MyBitdefender utilizando um endereço de e-mail que já não utiliza e pretende alterá-lo.

Não é possível alterar o endereço de e-mail, mas pode utilizar um endereço de e-mail diferente para criar uma nova conta online.

Para criar outra conta MyBitdefender com sucesso, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no ícone na parte superior da janela e selecione **Informações da Conta** no menu suspenso.

   Se já fez login a uma conta, a conta à qual está ligado é apresentada. Clique em **Iniciar sessão com outra conta** para alterar a conta ligada ao computador.

   Uma nova janela irá aparecer.

3. Clique em **Criar uma nova conta**.
4. Digite as informações necessárias nos campos correspondentes. Os dados que nos fornecer serão mantidos confidenciais.
   - **Email** - introduza o seu endereço de email.
   - **Nome de Utilizador** - insira um nome de utilizador para a sua conta.
   - **Palavra-passe** - digite a palavra-passe da sua conta. A palavra-passe deve ter pelo menos 6 caracteres de tamanho.
   - **Confirmar palavra-passe** - volte a introduzir a palavra-passe.
   - Clique em **Criar**.
5. Antes de poder usar a sua conta, deve concluir o registo. Verifique o seu email e siga as instruções no email de confirmação enviado pela Bitdefender.

Utilize o novo endereço de e-mail para iniciar sessão em MyBitdefender.

11.3. Como reponho a palavra-passe da conta MyBitdefender?

Para definir uma nova palavra-passe para a sua conta MyBitdefender, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no ícone na parte superior da janela e selecione **Informações da Conta** no menu suspenso.

   Uma nova janela irá aparecer.
3. Clique na hiperligação **Esqueci-me da palavra-passe**.
4. Digite o endereço de e-mail utilizado para criar a sua conta MyBitdefender e clique na hiperligação **Recuperar palavra-passe**.
5. Verifique o seu e-mail e clique na hiperligação fornecida.

   Uma nova janela irá aparecer.
6. Digite a nova palavra-passe. A palavra-passe deve ter pelo menos 6 caracteres de tamanho.
7. Introduza novamente a palavra-passe no campo **Introduza a palavra-passe novamente**.

8. Clique em **Submeter**.

Para aceder à sua conta MyBitdefender, digite o seu endereço de e-mail e a nova palavra-passe que acabou de definir.

12. A ANALISAR COM BITDEFENDER

12.1. Como posso analisar um ficheiro ou uma pasta?

A forma mais fácil para analisar um ficheiro ou pasta é clicar com o botão direito do rato no objeto a analisar, apontar para o Bitdefender e selecionar **Analisar com o Bitdefender** a partir do menu.

Para concluir a análise, siga o assistente de Análise Antivírus. O Bitdefender tomará automaticamente as ações recomendadas nos ficheiros detetados.

Se ainda houver ameaças não resolvidas, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas.

Situações típicas em que deve de usar este método de análise são as seguintes:

- Suspeita que um determinado ficheiro ou pasta está infectado.
- Sempre que descarrega da Internet ficheiros que julga serem perigosos.
- Quer analisar uma partilha de rede antes de copiar os ficheiros para o seu computador.

12.2. Como posso analisar o seu sistema?

Para realizar uma análise completa ao sistema, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. No módulo **Antivírus**, selecione a **Análise do Sistema**.
4. Siga o assistente de Análise Antivírus para completar a análise. O Bitdefender tomará automaticamente as ações recomendadas nos ficheiros detetados.

   Se ainda houver ameaças não resolvidas, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas. Para mais informação, por favor consulte o "*Assistente de Análise Antivírus*" (p. 99).

12.3. Como posso criar uma tarefa de análise personalizada?

Se quer analisar localizações específicas no seu computador ou configurar as opções de análise, pode configurar e executar uma tarefa personalizada.

Para criar uma tarefa de análise personalizada, proceda da seguinte forma:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. No módulo **Antivírus**, selecione **Gerir Análises**.
4. Clique em **Nova tarefa personalizada** para introduzir um nome para a análise e selecione as localizações a serem analisadas.
5. Se desejar configurar detalhadamente as opções de análise, selecione o separador **Avançado**.

   Pode facilmente configurar as opções de análise ajustando o nível de análise. Arraste o cursor pela escala para definir o nível de análise pretendido.

   Também pode optar por desligar o computador sempre que a análise termina, se não forem encontradas ameaças. Lembre-se de que esta será a ação por defeito sempre que executar esta tarefa.
6. Clique em **OK** para guardar as alterações e fechar a janela.
7. Clique em **Agendar** se pretender definir uma agenda para a sua tarefa de análise.
8. Clique em **Iniciar Análise** e siga o assistente de Análise Antivírus para completar a análise. No final da análise, será notificado para escolher as ações que devem ser tomadas nos ficheiros detetados, caso os haja.
9. Se quiser, pode voltar a executar rapidamente uma análise personalizada anterior ao clicar na entrada correspondente na lista disponível.

12.4. Como posso excluir uma pasta da análise?

O Bitdefender permite excluir ficheiros, pastas ou extensões de ficheiros específicos da análise.

As exceções devem ser usadas pelos utilizadores que possuem conhecimento informáticos avançados e apenas nas seguintes situações:

- Você tem uma pasta grande no seu sistema onde guarda filmes e música.
- Você tem um ficheiro grande no seu sistema onde guarda diferentes dados.
- Você tem uma pasta onde instala diferentes tipos de software e aplicações para testar. A análise da pasta pode resultar na perda de alguns dados.

Para adicionar uma pasta à lista de Exceções, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Antivírus**.
4. Na janela **Antivírus**, selecione o separador **Exceções**.
5. Assegure-se de que as **Exclusões ficheiros** está ligada através de clicar no botão.
6. Clique na ligação **Ficheiros e pastas excluídos**.
7. Clique no botão **Adicionar** , localizado no cimo da tabela de exceções.
8. Clique em **Explorar**, selecione a pasta que deseja excluir da análise e depois clique **OK**.
9. Clique em **Adicionar** e, em seguida, em **OK** para guardar as alterações e fechar a janela.

12.5. O que fazer se o Bitdefender identificar um ficheiro limpo como infectado?

Pode haver casos em que o Bitdefender assinala erradamente um ficheiro legítimo como sendo uma ameaça (um falso positivo). Para corrigir este erro, adicione o ficheiro à área de Exceções do Bitdefender:

1. Desative a proteção antivírus em tempo real do Bitdefender:
   a. Abra a janela de Bitdefender.
   b. Aceda ao painel de **Proteção**.
   c. Clique no módulo **Antivírus**.
   d. Na janela **Antivírus**, selecione o separador **Escudo**.
   e. Clique no botão para desligar **Análise no-acesso**.

Uma janela de aviso irá aparecer. Tem de confirmar a sua escolha seleccionando no menu durante quanto tempo pretende desactivar a protecção em tempo real. Pode desactivar a sua protecção em tempo-real durante 5, 15 ou 30 minutos, por uma hora, permanentemente ou até que o sistema reinicie.

2. Mostrar objetos ocultos no Windows. Para saber como fazer isto, consulte "*Como posso mostrar objetos ocultos no Windows?*" (p. 82).
3. Restaurar o ficheiro da área de Quarentena:
   a. Abra a janela de Bitdefender.
   b. Aceda ao painel de **Proteção**.
   c. Clique no módulo **Antivírus**.
   d. Na janela **Antivírus**, selecione o separador **Quarentena**.
   e. Selecione um ficheiro e clique em **Restaurar**.
4. Adicionar o ficheiro à lista de Exceções. Para saber como fazer isto, consulte "*Como posso excluir uma pasta da análise?*" (p. 62).
5. Ligue a proteção antivírus em tempo real do Bitdefender.
6. Contacte os nossos representantes do suporte para que possamos remover a assinatura de deteção. Para saber como fazer isto, consulte "*Pedir Ajuda*" (p. 227).

12.6. Como posso saber que vírus o Bitdefender detetou?

Cada vez que uma análise é levada a cabo, um registo de análise é criado e o Bitdefender regista as incidências detetadas.

O relatório da análise contém informação detalhada acerca dos processos de análise registados, tal como as opções da análise, o alvo da análise, as ameaças encontradas e as ações tomadas sobre essas ameaças.

Pode abrir o relatório diretamente no assistente de análise, assim que esta terminar, clicando em **Mostrar Relatório**.

Para analisar mais tarde um relatório de análise ou qualquer infeção detetada, siga estes passos:

1. Abra a janela de Bitdefender.

2. Clique no ícone na parte superior da janela e selecione **Definições Gerais** do menu suspenso.
3. Na janela **Eventos**, selecione **Antivírus** do menu suspenso correspondente.

   Aqui poderá encontrar todos os eventos de análise malware, incluindo ameaças detetadas na análise no acesso, análises iniciadas pelo utilizador e alterações de estado para as análises automáticas.
4. Na lista de eventos, pode ver as análises que foram recentemente efetuadas. Clique no evento para visualizar detalhes sobre o mesmo.
5. Para abrir um relatório da análise, clique em **Ver Relatório**. O registo da análise irá abrir numa nova janela.

13. CONTROLO PARENTAL

13.1. Como posso proteger os meus filhos de ameaças online?

O Controlo Parental Bitdefender permite-lhe restringir o acesso à Internet e a determinadas aplicações, impedindo os seus filhos de visualizarem conteúdos inapropriados sempre que não está por perto.

Para configurar o Controlo Parental, siga estes passos:

1. Criar uma conta do Windows limitada (standard) para a sua criança usar. Para mais informação, por favor consulte o "*Como posso criar contas de utilizador do Windows?*" (p. 69).
2. Certifique-se que tem a sessão iniciada com a conta de administrador. Apenas os utilizadores com direitos de administrador no sistema podem aceder e configurar o Controlo Parental.
3. Configure o Controlo Parental para as contas de utilizador do Windows que as suas crianças utilizam.
   a. Abra a janela de Bitdefender.
   b. Aceda ao painel de **Privacidade**.
   c. No módulo **Controlo Parental**, selecione **Configurar**.

      Certifique-se de que tem sessão iniciada na sua conta MyBitdefender.
   d. O painel do Controlo Parental abrirá numa nova janela. Áqui é o local onde poderá verificar e configurar as definições do Controlo Parental.
   e. Clique em **Adicionar Filho** do lado esquerdo do menu.
   f. Insira o nome e a idade do filho na barra **Perfil** A definição da idade da criança vai carregar automaticamente as definições consideradas adequadas para essa faixa etária, com base nos padrões de desenvolvimento infantil.

Verifique a atividade dos seus filhos e altere as definições do controlo Parental usando a MyBitdefender a partir de qualquer computador ou dispositivo móvel ligado à Internet.

Para informações mais detalhadas sobre como usar o Controlo Parental, por favor consulte "*Controlo Parental*" (p. 156).

13.2. Como posso restringir o acesso à Internet do meu filho?

Uma vez que tenha configurado o Controlo Parental, pode facilmente bloquear o acesso à internet durantes períodos de tempo determinados.

o Controlo Parental do Bitdefender permite-lhe controlar o uso da Internet por parte dos seus filhos mesmo quando não se encontra em casa.

Para restringir o acesso à Internet para determinadas horas do dia, faça o seguinte:

1. Em qualquer dispositivo com acesso à Internet, abra o navegador web.
2. Vá para:https://my.bitdefender.com
3. Inicie sessão na sua conta com o seu nome de utilizador e palavra-passe.
4. Clique em **Controlo Parental** para aceder ao painel.
5. Selecione o perfil do seu filho no lado esquerdo do menu.
6. Clique em no painel **Web** para aceder à janela de **Atividade Web**.
7. Clique em **Agendar**.
8. Selecione na grelha os intervalos de tempo em que o acesso à Internet está bloqueado. Pode clicar em células individuais, ou pode clicar e arrastar o rato para abranger períodos maiores.
9. Clique no botão **Guardar**.

Nota
O Bitdefender vai efetuar atualizações a cada hora independentemente de o acesso à Internet estar bloqueado.

13.3. Como bloqueio o acesso do meu filho a um website?

O Controlo Parental do Bitdefender permite-lhe controlar o tipo de conteúdo que é acedido pelo seu filho enquanto está a usar o seu computador e permite-lhe bloquear o acesso a um website mesmo que não esteja em casa.

Para bloquear o acesso a um site web, siga os seguintes passos:

1. Em qualquer dispositivo com acesso à Internet, abra o navegador web.

2. Vá para:https://my.bitdefender.com
3. Inicie sessão na sua conta com o seu nome de utilizador e palavra-passe.
4. Clique em **Controlo Parental** para aceder ao painel.
5. Selecione o perfil do seu filho no lado esquerdo do menu.
6. Clique em no painel **Web** para aceder à janela de **Atividade Web**.
7. Clique em **Lista negra/Lista branca**.
8. Insira o site web no respetivo campo.
9. Clique em **Bloquear** para adicionar o site Web à lista.
10. Selecione na grelha os intervalos de tempo em que o acesso é permitido. Pode clicar em células individuais, ou pode clicar e arrastar o rato para abranger períodos maiores.

    Clique no botão **OK**.
11. Se mudar de ideias, selecione o site Web e clique no botão **Remover** correspondente.

13.4. Como impeço o meu filho de jogar um jogo?

O Controlo Parental do Bitdefender permite-lhe controlar o conteúdo a que o seu filho acede quando usa o computador.

Se necessita de restringir o acesso a um jogo ou aplicação, pode usar o Controlo Parental do Bitdefender mesmo quando não está em casa.

Para bloquear o acesso a um jogo, siga estes passos:

1. Em qualquer dispositivo com acesso à Internet, abra o navegador web.
2. Vá para:https://my.bitdefender.com
3. Inicie sessão na sua conta com o seu nome de utilizador e palavra-passe.
4. Clique em **Controlo Parental** para aceder ao painel.
5. Selecione o perfil do seu filho no lado esquerdo do menu.
6. Clique no painél **Aplicações** para aceder à janela **Atividade Aplicações**.
7. Clique na **Lista Negra**.
8. Insira (ou copie e cole) o caminho para o executável no campo correspondente.

9. Clique em **Bloquear** para adicionar a aplicação a **Aplicações bloqueadas**.
10. Se mudar de ideias, clique no correspondente botão **Permitir**.

13.5. Como posso criar contas de utilizador do Windows?

Uma conta de utilizador do Windows é um perfil exclusivo que inclui todas as definições, os privilégios e os ficheiros pessoais de cada utilizador. As contas do Windows permitem ao administrador do PC controlar o acesso dos restantes utilizadores.

É muito útil definir contas de utilizador quando o computador é utilizado tanto por adultos como por crianças - um pai pode definir uma conta para cada filho.

Escolha o seu sistema operativo para saber como criar contas do Windows.

- **Windows XP:**
  1. Inicie sessão no seu computador como administrador.
  2. Clique em Iniciar, Painel de Controlo e, depois, em Contas de Utilizador.
  3. Clique em Criar uma nova conta.
  4. Escreva o nome do utilizador. Pode utilizar o nome completo, o primeiro nome ou um pseudónimo. Depois, clique em Seguinte.
  5. Para o tipo de conta, selecione Limitada, e depois, em Criar Conta. As contas limitadas são adequadas para crianças pois não permitem fazer alterações ao sistema ou instalar certas aplicações.
  6. A sua nova conta será criada e apresentada no ecrã Gerir Contas.
- **Windows Vista ou Windows 7:**
  1. Inicie sessão no seu computador como administrador.
  2. Clique em Iniciar, Painel de Controlo e, depois, em Contas de Utilizador.
  3. Clique em Criar uma nova conta.
  4. Escreva o nome do utilizador. Pode utilizar o nome completo, o primeiro nome ou um pseudónimo. Depois, clique em Seguinte.
  5. Para o tipo de conta, clique em Padrão e, depois, em Criar Conta. As contas limitadas são adequadas para crianças pois não permitem fazer alterações ao sistema ou instalar certas aplicações.

6. A sua nova conta será criada e apresentada no ecrã Gerir Contas.

- **Windows 8:**

1. Inicie sessão no seu computador como administrador.
2. Aponte o rato para o canto superior direito do ecrã, clique em Definições e, em seguida, clique em Alterar definições do PC.
3. Clique em Utilizadores no menu ao lado esquerdo e, em seguida, clique em Adicionar um utilizador.

   Pode criar uma conta Microsoft ou uma conta Local. Leia a descrição de cada tipo de conta e siga as instruções no ecrã para criar uma nova conta.

Nota
Agira que adicionou novas contas de utilizador, pode criar palavras-passe para as contas.

13.6. Como remover um perfil de criança

Caso pretenda remover um perfil de criança existente, siga estes passos:

1. Em qualquer dispositivo com acesso à Internet, abra o navegador web.
2. Vá para: https://my.bitdefender.com.
3. Inicie sessão na sua conta com o seu nome de utilizador e palavra-passe.
4. Clique em **Controlo Parental** para aceder ao painel.
5. Selecione o perfil da criança que pretende eliminar no menu do lado esquerdo.
6. Clique em **Definições de Conta**.
7. Clique em **Remover Perfil**.
8. Clique em **OK**.

14. PROTECÇÃO DE PRIVACIDADE

14.1. Como posso ter a certeza de que a minha transação online é segura?

Para ter a certeza de que as suas operações online se mantém privadas, pode usar o browser fornecido pelo Bitdefender para proteger as suas transações e as suas aplicações bancárias.

O Bitdefender Safepay™ é um navegador desenhado para proteger as informações do seu cartão de crédito, número de conta ou qualquer outro dado pessoal que possa utilizar enquanto acede a diferentes localizações online.

Para manter a sua atividade online segura e privada, faça o seguinte:

1. Abra a janela de Bitdefender.
2. Clique no botão **Safepay** à direita na janela.
3. Clique no ícone para aceder ao **Teclado Virtual**.
4. Use o **Teclado Virtual** quando inserir informação sensível tal como palavras-passe.

14.2. Como protejo a minha conta do Facebook?

Safego é uma aplicação do Facebook desenvolvida pelo Bitdefender para manter a sua conta da rede social segura.

O seu papel é analisar as hiperligações que recebe dos seus amigos do Facebook e monitorizar as suas definições de privacidade da conta.

Para aceder a Safego a partir do seu produto Bitdefender, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Ferramentas**.
3. No módulo **Safego**, selecione **Ativar para o Facebook**.

   Será direccionado para a sua conta.
4. Use a sua informação de acesso ao Facebook para aceder à aplicação Safego.

5. Permitir que Safego aceda à sua conta Facebook.

14.3. Como protejo a minha informação pessoal?

Para garantir que nenhum dado privado sai do seu computador sem o seu consentimento, você deve criar regras apropriadas de proteção de dados. As regras de proteção de dados especificam que a informação deve ser bloqueada.

Para criar uma regra de Proteção de Dados, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Privacidade**.
3. Clique no módulo de **Proteção de Dados**.
4. Se a **Proteção de Dados** estiver desligada, ative-a usando o botão adequado.
5. Selecione a opção **Adicionar regra** para iniciar o assistente Proteção de Dados.
6. Siga os passos do assistente.

14.4. Como removo um ficheiro permanentemente com o Bitdefender?

Se deseja remover um ficheiro permanentemente do seu sistema, necessita de pagar a informação fisicamente do seu disco duro.

O Destruidor de Ficheiros do Bitdefender pode ajudá-lo a rapidamente destruir ficheiros ou pastas do seu computador usando o menu contextual Windows, seguindo os seguintes passos:

1. Clique com o botão direito do rato no ficheiro ou pasta que deseja apagar permanentemente, e aponte para o Bitdefender e selecione **Destruidor de Ficheiros**.
2. A janela de confirmação irá aparecer. Clique em **Sim** para iniciar o assistente do Destruidor de Ficheiros.
3. Aguarde que o Bitdefender termine a destruição dos ficheiros.
4. Os resultados são apresentados. Clique em **Fechar** para sair do assistente.

15. TUNEUP

15.1. Como posso usar melhorar o desempenho do meu sistema?

O desempenho do sistema não depende apenas das características do hardware, tais como a capacidade do CPU, a memória disponível e o espaço no disco rígido. Está, também, diretamente relacionada com a configuração do software e com a gestão dos dados.

Estas são as ações principais que pode efetuar com o Bitdefender para melhorar a velocidade e o desempenho do seu sistema:

- "*Desfragmente o seu disco rígido*" (p. 73)
- "*Otimize o desempenho do seu sistema com um único clique*" (p. 73)
- "*Analise o seu sistema periodicamente*" (p. 74)

15.1.1. Desfragmente o seu disco rígido

Recomenda-se a desfragmentação do disco rígido, para aceder aos ficheiros mais depressa e melhorar o desempenho geral do sistema. O Desfragmentador do Disco ajuda a reduzir a fragmentação de ficheiros e melhora o desempenho do seu sistema.

Para iniciar o Desfragmentador do Disco, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Ferramentas**.
3. No painel **TuneUp**, selecione o **Desfragmentador de Disco**.
4. Siga os passos do assistente.

Para obter mais informações sobre o módulo de Desfragmentação de Disco, consulte "*Desfragmentar volumes de discos rígidos*" (p. 178).

15.1.2. Otimize o desempenho do seu sistema com um único clique

A opção Otimizador de Um Clique poupa-lhe quando quer uma maneira rápida de melhorar o desempenho do sistema ao analisar, detectar e limpar rapidamente ficheiros inúteis.

Para iniciar o processo Otimizador de Um Clique, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Ferramentas**.
3. No módulo **TuneUp**, selecione **Otimizador de Um Clique**.
4. Deixe que o Bitdefender procure ficheiros que possam ser eliminados, depois clique no botão **Otimizar** para concluir o processo.

Ou mais rápido, clique no botão **Otimizar** da interface do Bitdefender.

Para mais informações sobre como pode melhorar a velocidade do seu computador com um único clique, consulte "*A otimizar a velocidade do seu sistema com apenas um clique*" (p. 174).

15.1.3. Analise o seu sistema periodicamente

A velocidade do seu sistema e o seu comportamento geral também podem ser afectados pelo malware.

Certifique-se de que analisa o seu sistema periodicamente, pelo menos uma vez por semana.

Recomenda-se a utilização da Análise do Sistema pois a mesma analisa todos os tipos de malware que estejam a ameaçar a segurança do seu sistema e também analisa dentro dos ficheiros.

Para iniciar a Análise do Sistema, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. No módulo **Antivírus**, selecione a **Análise do Sistema**.
4. Siga os passos do assistente.

15.2. Como posso melhorar o tempo de arranque do meu sistema?

As aplicações desnecessárias que deixam o tempo de inicialização irritantemente mais lento quando abre o seu PC podem ter a sua abertura desativada ou adiada com o Otimizador de Inicialização, poupando-lhe, assim, tempo valioso.

Para utilizar o Otimizador de Arranque, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Ferramentas**.
3. No módulo **TuneUp**, selecione **Otimizador de Arranque**.
4. Selecione as aplicações que quer adiar no arranque do sistema.

Para mais informações sobre como otimizar o tempo de arranque do seu PC, consulte *"A otimizar o tempo de arranque do seu PC."* (p. 175).

16. INFORMAÇÕES ÚTEIS

16.1. Como testo a minha solução antivírus?

Para garantir que o seu produto Bitdefender está a funcionar corretamente, recomendamos a utilização do teste Eicar.

O teste Eicar permite que verifique a sua proteção antivírus utilizando um ficheiro de segurança desenvolvido para este fim.

Para testar a sua solução antivírus, siga estes passos:

1. Transfira o teste da página Web oficial da organização EICAR http://www.eicar.org/.
2. Clique no separador **Ficheiro de teste antimalware**.
3. Clique em **Transferir** no menu do lado esquerdo.
4. A partir da **área de transferência utilizando o protocolo padrão http** clique no ficheiro de teste **eicar.com**.
5. Receberá informações de que a página a que está a tentar aceder contém o Ficheiro de Teste EICAR (não é um vírus).

   Caso clique em **Compreendo os riscos, leve-me até lá mesmo assim**, a transferência do teste irá iniciar e um pop-up do Bitdefender irá informá-lo da deteção de um vírus.

   Clique em **Mais Detalhes** para obter mais informações sobre esta ação.

Caso não receba qualquer alerta de Bitdefender, recomendamos que entre em contacto com Bitdefender para suporte conforme descrito na secção "*Pedir Ajuda*" (p. 227).

16.2. Como posso remover o Bitdefender?

Caso pretenda remover o Bitdefender Internet Security 2015, siga os seguintes passos:

- No **Windows XP**:
  1. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Adicionar/Remover Programas**.
  2. Encontre o **Bitdefender Internet Security 2015** e selecione **Remover**.
  3. Clique em **Remover** para continuar.

4. Neste passo tem as seguintes opções:
   - **Eu quero reinstalá-lo** - irá remover completamente o Bitdefender. O Verificador de Vírus em 60 segundos do Bitdefender não será instalado.
   - **Eu quero removê-lo permanentemente** - irá remover completamente o Bitdefender. O Verificador de Vírus em 60 segundos do Bitdefender será instalado no seu sistema para o proteger contra malware.

   Selecione a opção pretendida e clique em **Seguinte**.
5. Aguarde que o processo de desinstalação conclua e, em seguida, reinicie o sistema.

- No **Windows Vista** e **Windows 7**:
  1. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.
  2. Encontre o **Bitdefender Internet Security 2015** e selecione **Desinstalar**.
  3. Clique em **Remover** para continuar.
  4. Neste passo tem as seguintes opções:
     - **Eu quero reinstalá-lo** - irá remover completamente o Bitdefender. O Verificador de Vírus em 60 segundos do Bitdefender não será instalado.
     - **Eu quero removê-lo permanentemente** - irá remover completamente o Bitdefender. O Verificador de Vírus em 60 segundos do Bitdefender será instalado no seu sistema para o proteger contra malware.

     Selecione a opção pretendida e clique em **Seguinte**.
  5. Aguarde que o processo de desinstalação conclua e, em seguida, reinicie o sistema.
- No **Windows 8**:
  1. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
  2. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.
  3. Encontre o **Bitdefender Internet Security 2015** e selecione **Desinstalar**.
  4. Clique em **Remover** para continuar.

5. Neste passo tem as seguintes opções:
   - **Eu quero reinstalá-lo** - irá remover completamente o Bitdefender. O Verificador de Vírus em 60 segundos do Bitdefender não será instalado.
   - **Eu quero removê-lo permanentemente** - irá remover completamente o Bitdefender. O Verificador de Vírus em 60 segundos do Bitdefender será instalado no seu sistema para o proteger contra malware.

   Selecione a opção pretendida e clique em **Seguinte**.
6. Aguarde que o processo de desinstalação conclua e, em seguida, reinicie o sistema.

Nota
O Verificador de Vírus em 60 segundos do Bitdefender é uma aplicação livre que utiliza a tecnologia de análise na nuvem para detetar programas maliciosos e ameaças em menos de 60 segundos.

16.3. Como mantenho o meu sistema protegido após a desinstalação do Bitdefender?

Durante o processo de remoção do Bitdefender Internet Security 2015, tem a opção **Eu quero removê-lo permanentemente** com a possibilidade de instalar o Verificador de Vírus em 60 segundos do Bitdefender no seu sistema.

O Verificador de Vírus em 60 segundos do Bitdefender é uma aplicação livre que utiliza a tecnologia de análise na nuvem para detetar programas maliciosos e ameaças em menos de 60 segundos.

Pode continuar a utilizar a aplicação mesmo se reinstalar o Bitdefender ou se instalar outro programa antivírus no sistema.

Se pretende remover o Verificador de Vírus em 60 segundos do Bitdefender, siga estes passos:

- No **Windows XP**:
  1. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Adicionar/Remover Programas**.
  2. Encontre **Verificador de Vírus em 60 segundos do Bitdefender** e selecione **Remover**.

3. Selecione **Desinstalar** no próximo passo e aguarde pela conclusão do processo.

- No **Windows Vista** e **Windows 7**:

  1. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.
  2. Encontre **Verificador de Vírus em 60 segundos do Bitdefender** e selecione **Desinstalar**.
  3. Selecione **Desinstalar** no próximo passo e aguarde pela conclusão do processo.

- No **Windows 8**:

  1. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
  2. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.
  3. Selecione **Verificador de Vírus em 60 segundos do Bitdefender** e clique em **Desinstalar**.
  4. Selecione **Desinstalar** no próximo passo e aguarde pela conclusão do processo.

16.4. Como desligo automaticamente o meu computador após terminar a análise?

O Bitdefender oferece múltiplas tarefas de análise que pode usar para se certificar que o seu sistema não está infectado com malware. Analisar todo o computador pode levar muito mais tempo a completar dependendo do hardware do seu sistema e da configuração do seu software.

Por essa razão, o Bitdefender permite-lhe configurar o Bitdefender para desligar o computador assim que a análise terminar.

Por exemplo: terminou de trabalhar no seu computador e deseja ir dormir. Gostava de ter o seu sistema completamente analisado em busca de malware pelo Bitdefender.

Eis como define o Bitdefender para desligar o seu computador no final da análise:

1. Abra a janela de Bitdefender.

2. Aceda ao painel de **Proteção**.
3. No módulo **Antivírus**, selecione **Gerir Análises**.
4. Na janela **Gerir Tarefa de Análise**, clique em **Nova tarefa personalizada** para introduzir um nome para a análise e selecione os locais a serem analisados.
5. Se desejar configurar detalhadamente as opções de análise, selecione o separador **Avançado**.
6. Opte por desligar o computador sempre que a análise terminar e se não forem encontradas ameaças.
7. Clique em **OK** para guardar as alterações e fechar a janela.
8. Clique em **Iniciar Análise**.

Se não forem encontradas ameaças, o computador desliga-se.

Se ainda houver ameaças não resolvidas, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas. Para mais informação, por favor consulte o "*Assistente de Análise Antivírus*" (p. 99).

16.5. Como posso configurar Bitdefender para usar um proxy de ligação à Internet?

Se o seu computador se ligar a Internet através de um servidor proxy, você deve configurar as definições do proxy do Bitdefender. Normalmente, o Bitdefender deteta e importa automaticamente as definições proxy do seu sistema.

Importante

As ligações à internet domésticas normalmente não usam um servidor proxy. Como regra de ouro, verifique e configure as definições da ligação proxy do seu programa Bitdefender quando as atualizações não funcionam. Se o Bitdefender atualizar, então está corretamente configurado à Internet.

Para gerir as definições de proxy, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Clique no ícone na parte superior da janela e selecione **Definições Gerais** do menu suspenso.
3. Na janela **Definições Gerais** selecione a barra **Avançadas**.

4. Ative o uso de proxy clicando no botão.
5. Clique na ligação **Gerir proxies**.
6. Existem duas opções para as definições do proxy:
   - **Importe as definições de proxy do navegador por defeito** - as definições de proxy do utilizador actual, extraídas do explorador por defeito. Se o servidor proxy requer um nome de utilizador e uma palavra-passe, deverá inseri-los nos campos correspondentes.

     Nota
     O Bitdefender pode importar as definições de proxy dos navegadores mais populares, incluindo as versões mais recentes de Internet Explorer, Mozilla Firefox e Opera.

   - **Definições de proxy personalizadas** - definições de proxy que você pode configurar. As seguintes definições devem ser especificadas:
     - **Endereço** - introduza o IP do servidor proxy.
     - **Porta** - insira a porta que o Bitdefender usa para se ligar ao servidor proxy.
     - **Nome de Utilizador** - introduza um nome de utilizador reconhecido pelo proxy.
     - **Palavra-passe** - introduza uma palavra-passe válida para o utilizador previamente definido.
7. Clique em **OK** para guardar as alterações e fechar a janela.

O Bitdefender usará as definições de proxy disponíveis até conseguir ligar à Internet.

16.6. Estou a utilizar uma versão de 32 ou 64 Bit do Windows?

Para saber se tem um sistema operativo de 32 bit ou 64 bit, siga os seguintes passos:

- No **Windows XP**:
  1. Clique em **Iniciar**.
  2. Localize o **Meu Computador** no menu **Iniciar**.
  3. Clique com o botão direito em **Meu Computador** e selecione **Propriedades**.

4. Se estiver indicada a **Edição x64** na secção **Sistema**, está a executar a versão de 64 bit do Windows XP.

   Se não estiver indicada a **Edição x64**, está a executar a versão de 32 bit do Windows XP.

- No **Windows Vista** e **Windows 7**:

  1. Clique em **Iniciar**.
  2. Localize o **Computador** no menu **Iniciar**.
  3. Clique com o botão direito em **Computador** e selecione **Propriedades**.
  4. Procure na secção **Sistema** a informação sobre o seu sistema.

- No **Windows 8**:

  1. A partir do ecrã Iniciar do Windows, localize **Computador** (por exemplo, pode começar a digitar "Computador" diretamente no menu Iniciar) e, em seguida, clique com o botão direito do rato no seu ícone.
  2. Selecione **Propriedades** no menu inferior.
  3. Procure em **Sistema** o tipo de sistema.

16.7. Como posso mostrar objetos ocultos no Windows?

Estes passos são úteis nos casos de malware e tiver de encontrar e remover os ficheiros infectados, que poderão estar ocultos.

Siga os seguintes passos para mostrar objetos ocultos no Windows:

1. Clique em **Iniciar**, aceda ao **Painel de Controlo**.

   No **Windows 8**: A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
2. Selecione **Opções de Pastas**.
3. Abra o separador **Ver**.
4. Selecione **Mostrar conteúdo das pastas de sistema** (apenas para o Windows XP).
5. Selecione **Mostrar ficheiros e pastas ocultos**.
6. Desmarque **Ocultar extensões nos tipos de ficheiro conhecidos**.
7. Desmarque **Ocultar ficheiros protegidos do sistema operativo**.

8. Clique em **Aplicar** e depois em **OK**.

16.8. Como posso remover outras soluções de segurança?

A principal razão para utilizar uma solução de segurança é proporcionar proteção e segurança aos seus dados. Mas o que acontece quando tem mais do que um produto de segurança no mesmo sistema?

Quando utiliza mais do que uma solução de segurança no mesmo computador, o sistema torna-se instável. O instalador do Bitdefender Internet Security 2015 deteta automaticamente outros programas de segurança e oferece-lhe a opção de os desinstalar.

Se não tiver removido as outras soluções de segurança durante a instalação inicial, siga os seguintes passos:

- No **Windows XP**:
  1. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Adicionar/Remover Programas**.
  2. Aguarde alguns momentos até que a lista do software instalado seja apresentada.
  3. Encontre o nome do programa que pretende remover e selecione **Remover**.
  4. Aguarde que o processo de desinstalação conclua e, em seguida, reinicie o sistema.
- No **Windows Vista** e **Windows 7**:
  1. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.
  2. Aguarde alguns momentos até que a lista do software instalado seja apresentada.
  3. Encontre o nome do programa que pretende remover e selecione **Desinstalar**.
  4. Aguarde que o processo de desinstalação conclua e, em seguida, reinicie o sistema.
- No **Windows 8**:

1. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
2. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.
3. Aguarde alguns momentos até que a lista do software instalado seja apresentada.
4. Encontre o nome do programa que pretende remover e selecione **Desinstalar**.
5. Aguarde que o processo de desinstalação conclua e, em seguida, reinicie o sistema.

Se não conseguir remover as outras soluções de segurança do seu sistema, obtenha a ferramenta de desinstalação do site Internet do fornecedor ou contacte-o diretamente para receber instruções de desinstalação.

16.9. Como posso usar o Restauro do Sistema no Windows?

Se não conseguir iniciar o computador no modo normal, pode arrancar no Modo de Segurança e usar o Restauro do Sistema para o restaurar para um momento em que conseguia iniciar o computador sem erros.

Para executar o Restauro do Sistema, deve ter sessão iniciada no Windows como administrador.

Para usar o Restauro do Sistema, siga os seguintes passos:

- No **Windows XP**:
  1. Inicie o Windows no Modo de Segurança.
  2. Siga este caminho a partir do menu iniciar do Windows: **Iniciar** → **Todos os Programas** → **Ferramentas do Sistema** → **Restauro do Sistema**.
  3. Na página **Benvindo ao Restauro do Sistema**, clique para selecionar a opção **Restaurar o meu computador para um momento anterior** e depois clique em Seguinte.
  4. Siga os passos do assistente e deverá ser capaz de reiniciar o sistema no modo normal.
- No **Windows Vista** e **Windows 7**:
  1. Inicie o Windows no Modo de Segurança.

2. Siga este caminho a partir do menu iniciar do Windows: **Todos os Programas** → **Acessórios** → **Ferramentas do Sistema** → **Restauro do Sistema**.
3. Siga os passos do assistente e deverá ser capaz de reiniciar o sistema no modo normal.

- No **Windows 8**:
  1. Inicie o Windows no Modo de Segurança.
  2. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
  3. Selecione **Recuperação** e, em seguida, **Abrir restauro do sistema**.
  4. Siga os passos do assistente e deverá ser capaz de reiniciar o sistema no modo normal.

16.10. Como posso reiniciar no Modo de Segurança?

O Modo de Segurança é um modo operativo de diagnóstico, utilizado principalmente para detetar e resolver problemas que estejam a afetar o funcionamento normal do Windows. As causas destes problemas vão desde a incompatibilidade de controladores a vírus que impedem o arranque normal do Windows. No Modo de Segurança funcionam apenas algumas aplicações e o Windows só carrega os controladores básicos e os componentes mínimos do sistema operativo. É por isso que a maioria dos vírus está inativa quando o Windows está no Modo de Segurança e podem ser facilmente removidos.

Para iniciar o Windows no Modo de Segurança:

1. Reinicie o computador.
2. Prima a tecla **F8** várias vezes antes de o Windows iniciar para aceder ao menu de arranque.
3. Selecione **Modo Seguro** no menu de inicialização ou **Modo Seguro com Rede** se quiser ter acesso à Internet.
4. Prima em **Enter** e aguarde enquanto o Windows carrega o Modo Seguro.
5. Este processo termina com uma mensagem de confirmação. Clique em **OK** para aceitar.
6. Para iniciar o Windows normalmente, basta reiniciar o sistema.

GERIR A SUA SEGURANÇA

17. PROTEÇÃO ANTIVÍRUS

Bitdefender protege o seu computador de todo o tipo de malware (vírus, Trojans, spyware, rootkits e por aí fora). A proteção que Bitdefender oferece está dividida em duas categorias:

- Análise no acesso - previne que novas ameaças de malware entrem no seu sistema. Poe exemplo, Bitdefender irá analisar um documento word em busca de ameaças conhecidas quando você o abrir, e uma mensagem de e-mail quando recebe uma.

  A análise no acesso garante proteção em tempo real contra malware, sendo um componente essencial de qualquer programa informático de segurança.

  Importante
  Para prevenir a infecção de vírus no seu computador, mantenha ativada a **análise no acesso**.

- Análise a-pedido - permite detetar e remover malware que já se encontra a residir no seu sistema. Esta é uma análise clássica iniciada pelo utilizador – você escolhe qual a drive, pasta ou ficheiro o Bitdefender deverá analisar, e o mesmo é analisado – a-pedido.

O Bitdefender analisa automaticamente qualquer média removível que esteja ligado ao computador para garantir um acesso em segurança. Para mais informação, por favor consulte o "*Análise automática de média removíveis*" (p. 103).

Os utilizadores avançados podem configurar as exceções da análise se não quiserem que certos ficheiros ou tipos de ficheiros sejam analisados. Para mais informação, por favor consulte o "*Configurar exceções da análise*" (p. 105).

Quando deteta um vírus ou outro malware, o Bitdefender irá tentar remover automaticamente o código de malware do ficheiro e reconstruir o ficheiro original. Esta operação é designada por desinfecção. Os ficheiros que não podem ser desinfectados são movidos para a quarentena de modo a conter a infecção. Para mais informação, por favor consulte o "*Gerir ficheiros da quarentena*" (p. 107).

Se o seu computador estiver infectado com malware, por favor consulte "*Remover malware do seu sistema*" (p. 215). Para o ajudar a limpar o malware

do computador que não pode ser removido no sistema operativo Windows, o Bitdefender proporciona-lhe o Modo de Recuperação. Este é um ambiente fiável, concebido sobretudo para a remoção de malware, que lhe permite arrancar o seu computador independentemente do Windows. Quando o computador estiver a ser executado no Modo de Recuperação, o malware do Windows está inativo, tornando-se mais fácil a sua remoção.

Para o proteger contra aplicações desconhecidas maliciosas, o Bitdefender usa o Controlo Ativo de Vírus, uma tecnologia heurística avançada, a qual monitoriza continuamente as aplicações executadas no seu sistema. O Controlo Ativo de Vírus bloqueia automaticamente aplicações que exibem comportamento semelhante a malware para as impedir de danificar o seu computador. Ocasionalmente, as aplicações legítimas podem ser bloqueadas. Em tais situações, pode configurar o Controlo Activo de Vírus para não bloquear aquelas aplicações de novo criando regras de exclusão. Para saber mais, por favor consulte "*Controlo Ativo de Vírus*" (p. 108).

17.1. Análise no acesso (proteção em tempo real)

O Bitdefender fornece uma proteção contínua e em tempo real contra uma gama de ameaças de malware ao analisar todos os ficheiros acedidos e mensagens de e-mail.

As predefinições da proteção em tempo real asseguram uma ótima proteção contra malware, com um impacto mínimo no desempenho do seu sistema. Pode alterar facilmente as definições da proteção em tempo real de acordo com as suas necessidades mudando para um dos níveis de proteção predefinidos. Ou, no modo avançado, pode configurar as definições de análise em detalhe criando um nível de proteção personalizado.

17.1.1. Ligar ou desligar a proteção em tempo real

Para ativar ou desativar a proteção em tempo real contra o malware, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Antivírus**.
4. Na janela **Antivírus**, selecione o separador **Escudo**.
5. Clique no botão para ativar ou desativar a análise no acesso.

6. Se deseja desativar a Proteção em Tempo-real, uma janela de aviso irá aparecer. Tem de confirmar a sua escolha seleccionando no menu durante quanto tempo pretende desactivar a protecção em tempo real. Pode desactivar a sua protecção em tempo-real durante 5, 15 ou 30 minutos, por uma hora, permanentemente ou até que o sistema reinicie. A proteção em tempo real será ativada automaticamente quando o tempo selecionado expirar.

Atenção
Esta é uma incidência de segurança critica. Recomendamos que desactive a protecção em tempo-real o menos tempo possível. Quando a mesma está desactivada você deixa de estar protegido contra as ameaças do malware.

17.1.2. Ajustar o nível de proteção em tempo real

O nível de proteção em tempo real determina as definições de análise da proteção em tempo real. Pode alterar facilmente as definições da proteção em tempo real de acordo com as suas necessidades mudando para um dos níveis de proteção predefinidos.

Para ajustar o nível de proteção em tempo real, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Antivírus**.
4. Na janela **Antivírus**, selecione o separador **Escudo**.
5. Arraste o cursor pela escala para definir o nível de proteção pretendido. Utilize a descrição do lado direito da escala para escolher o nível de proteção que melhor se adequa às suas necessidades de segurança.

17.1.3. Configurar as definições da proteção em tempo-real

Os utilizadores avançados podem aproveitar as definições que o Bitdefender oferece. Pode configurar as definições da proteção em tempo real criando um nível de proteção personalizado.

Para configurar as definições da proteção em tempo-real, siga os seguintes passos:

1. Abra a janela de Bitdefender.

2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Antivírus**.
4. Na janela **Antivírus**, selecione o separador **Escudo**.
5. Clique em **Personalizar**.
6. Configure as definições de análise como necessário.
7. Clique em **OK** para guardar as alterações e fechar a janela.

Informação sobre as opções de análise

Poderá achar esta informação útil:

- Se não está familiarizado com alguns dos termos, procure-os no glossário. Pode também encontrar informação útil pesquisando a Internet.
- **Opções de análise para ficheiros acedidos.** Pode configurar o Bitdefender para analisar todos os ficheiros ou apenas aplicações (ficheiros de programas) acedidos. A análise de todos os ficheiros acedidos proporciona uma maior segurança, enquanto a análise apenas das aplicações pode ser utilizada para melhorar o desempenho do sistema.

  Por defeito, ambas as pastas locais e partilhas de rede são sujeitas a análise no acesso. Para um melhor desempenho do sistema, pode excluir os locais de rede da análise no acesso.

  As aplicações (ou ficheiros de programa) são muito mais vulneráveis a ataques de malware do que qualquer outro tipo de ficheiros. Esta categoria inclui as seguintes extensões de ficheiro:

  386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Analisar dentro dos arquivos.** Analisar o interior de arquivos é um processo lento e que consome muitos recursos, não sendo, por isso recomendado para a proteção em tempo real. Os arquivos que contém ficheiros infectados não são uma ameaça imediata à segurança do seu sistema. O malware só pode afetar o seu sistema se o ficheiro infectado for extraído do arquivo e executado sem que a proteção em tempo real esteja ativada.

  Se decidir usar esta opção, pode definir um tamanho limite aceitável para os ficheiros analisados no acesso. Selecione a caixa de seleção correspondente e digite o tamanho máximo do ficheiro (em MB).

- **Opções de análise para e-mail e Internet.** Para impedir que seja transferido malware para o seu computador, o Bitdefender analisa automaticamente os seguintes pontos de entrada de malware:
  - emails recebidos e enviados
  - tráfego da Internet

  Analisar o tráfego na Internet poderá abrandar um pouco a navegação, mas vai bloquear o malware proveniente da Internet, incluindo transferências "drive-by".

  Apesar de não ser recomendado, pode desativar a análise do antivírus de e-mail ou da Internet para aumentar o desempenho do sistema. Se desativar as respetivas opções de análise, as mensagens eletrónicas e os ficheiros recebidos e transferidos da Internet não serão analisados, permitindo que ficheiros infectados sejam guardados no seu computador. Esta é uma ameaça grave pois a proteção em tempo real vai bloquear o malware quando os ficheiros infectados forem acedidos (abertos, movidos, copiados ou executados).

- **Analisar sectores de arranque.** Pode definir o Bitdefenderpara analisar os sectores de saída do seu disco rígido. Este sector do disco rígido contém o código do computadores necessário para iniciar o processo de reinício. Quando um vírus infecta o sector de saída, a drive pode tornar-se inacessível ou poderá não conseguir iniciar o seu sistema e aceder aos seus dados.

- **Analisar só ficheiros alterados.** Ao analisar apenas ficheiros novos e modificados, pode melhorar significativamente o desempenho do seu sistema sem comprometer a sua segurança.

- **Analisar em busca de Keyloggers.** Selecione esta opção para analisar o seu sistema em busca de aplicações keylogger. Os keyloggers gravam o que você digita no seu teclado e enviam relatórios pela Internet para uma

pessoa maliciosa (hacker). O hacker pode descobrir informação sensível a partir de dados roubados, tais como números de contas bancárias e palavras-passe, e usá-las em benefício pessoal.

Ações tomadas em malware detetado

Pode configurar as ações a serem levadas a cabo pela proteção em tempo-real.

Para configurar as ações, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Antivírus**.
4. Na janela **Antivírus**, selecione o separador **Escudo**.
5. Clique em **Personalizar**.
6. Configure as definições de análise como necessário.
7. Clique em **OK** para guardar as alterações e fechar a janela.

As seguintes ações podem ser levadas a cabo pela proteção em tempo-real do Bitdefender:

Tomar ações adequadas

Bitdefender tomará as ações recomendadas dependendo do tipo de ficheiro detetado:

- **Ficheiros infectados.** Os ficheiros detetados como infectados correspondem a uma assinatura de malware na Base de Dados de Assinaturas de Malware do Bitdefender. Bitdefender tentará automaticamente remover o código malware do ficheiro infetado e reconstruir o ficheiro original. Esta operação é designada por desinfecção.

  Os ficheiros que não podem ser desinfectados são movidos para a quarentena de modo a conter a infecção. O ficheiros em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece. Para mais informação, por favor consulte o "*Gerir ficheiros da quarentena*" (p. 107).

Importante
Para determinados tipos de malware, a desinfecção não é possível por o ficheiro detectado ser totalmente malicioso. Nestes casos, o ficheiro infectado é eliminado do disco.

- **Ficheiros suspeitos.** Os ficheiros são detetados como suspeitos pela análise heurística. Não foi possível desinfectar os ficheiros suspeitos por não estar disponível uma rotina de desinfecção. Serão movidos para a quarentena para evitar uma potencial infeção.

  Por defeito, os ficheiros da quarentena são automaticamente enviados para os Laboratórios Bitdefender para serem analisados pelos investigadores de malware da Bitdefender. Se a presença de malware for confirmada, é emitida uma assinatura para possibilitar a remoção do malware.

- **Aquivos que contêm ficheiros infetados.**
  - Os arquivos que contêm apenas ficheiros infetados são eliminados automaticamente.
  - Se um arquivo tiver ficheiros infectados e limpos, o Bitdefender tentará eliminar os ficheiros infectados desde que possa reconstruir o arquivo com os ficheiros limpos. Se não for possível a reconstrução do arquivo, será informado de que não pode ser tomada qualquer ação, de forma a evitar perder ficheiros limpos.

Mover ficheiros para a Quarentena
Move os ficheiros infectados para a quarentena. O ficheiros em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece. Para mais informação, por favor consulte o "*Gerir ficheiros da quarentena*" (p. 107).

Negar acesso
Será negado o acesso de um ficheiro que se encontre infectado.

17.1.4. Restaurar as predefinições

As predefinições da proteção em tempo real asseguram uma ótima proteção contra malware, com um impacto mínimo no desempenho do seu sistema.

Para restaurar as definições da proteção em tempo real, siga os seguintes passos:

1. Abra a janela de Bitdefender.

2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Antivírus**.
4. Na janela **Antivírus**, selecione o separador **Escudo**.
5. Clique em **Predefinição**.

17.2. Verificação por ordem

O objectivo principal do Bitdefender é manter o seu computador livre de vírus. Isto é feito ao manter os novos vírus fora do seu computador e ao analisar as suas mensagens de e-mail e quaisquer novos ficheiros transferidos ou copiados para o seu sistema.

Há o risco de o vírus já ter acedido ao seu sistema, antes mesmo de ter instalado o Bitdefender. Este é o motivo, pelo qual é uma excelente ideia verificar vírus residentes no seu computador depois de instalar o Bitdefender. E é definitivamente uma boa ideia, analisar frequentemente o seu computador em busca de vírus.

A análise a-pedido está baseada em tarefas de análise. As tarefas de análise especificam as opções de análise e os objectos a serem analisados. Pode analisar o computador sempre que quiser executar as tarefas por defeito ou as suas próprias tarefas de análise (tarefas definidas pelo utilizador). Se quer analisar localizações específicas no seu computador ou configurar as opções de análise, pode configurar e executar uma análise personalizada.

17.2.1. Procurar malware num ficheiro ou pasta

Deve analisar os ficheiros e as pastas sempre que suspeitar de uma infecção. Clique com o botão direito do rato sobre o ficheiro ou pasta que pretende analisar, aponte para o **Bitdefender** e selecione **Analisar com o Bitdefender**. O Assistente de Análise Antivírus irá surgir e guiá-lo através do processo de análise. No final da análise, será notificado para escolher as ações que devem ser tomadas nos ficheiros detetados, caso os haja.

17.2.2. Executar uma Análise Rápida

A Análise Rápida utiliza a análise nas nuvens para detetar malware em execução no seu sistema. Normalmente, a realização de uma Análise Rápida demora menos de um minuto e utiliza uma fação dos recursos do sistema necessários para uma análise de vírus normal.

Para executar uma Análise Rápida, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. No módulo **Antivírus**, selecione **Análise Rápida**.
4. Siga o assistente de Análise Antivírus para completar a análise. O Bitdefender tomará automaticamente as ações recomendadas nos ficheiros detetados. Se ainda houver ameaças não resolvidas, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas.

17.2.3. Executar uma Análise do Sistema

A tarefa de Análise do Sistema procura em todo o computador todos os tipos de malware que ameaçam a sua segurança, tais como vírus, spyware, adware, rookits e outros.

Nota
Porque a **Análise do Sistema** leva a cabo uma análise minuciosa de todo o seu computador, a mesma poderá levar algum tempo. Portanto, recomenda-se que execute esta tarefa quando não estiver a usar o seu computador.

Antes de executar uma Análise do Sistema, recomendamos o seguinte:

- Certifique-se de que o Bitdefender apresenta as assinaturas de malware actualizadas. Analisar o seu computador usando assinaturas desactualizadas pode impedir que o Bitdefender detecte novo malware encontrado desde a última actualização. Para mais informação, por favor consulte o "*Mantenha o seu Bitdefender atualizado.*" (p. 44).
- Encerre todos os programas abertos.

Se quer analisar localizações específicas no seu computador ou configurar as opções de análise, pode configurar e executar uma análise personalizada. Para mais informação, por favor consulte o "*Configurar uma análise personalizada*" (p. 96).

Para levar a cabo uma Análise do Sistema, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. No módulo **Antivírus**, selecione a **Análise do Sistema**.

4. Siga o assistente de Análise Antivírus para completar a análise. O Bitdefender tomará automaticamente as ações recomendadas nos ficheiros detetados. Se ainda houver ameaças não resolvidas, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas.

17.2.4. Configurar uma análise personalizada

Para configurar uma análise ao malware em detalhe e depois executá-la, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. No módulo **Antivírus**, selecione **Gerir Análises**.
4. Clique em **Nova tarefa personalizada**. Insira um nome para a análise na aba **Básico** e selecione as localizações a serem analisadas.
5. Se desejar configurar detalhadamente as opções de análise, selecione o separador **Avançado**. Uma nova janela irá aparecer. Siga os seguintes passos:
   a. Pode facilmente configurar as opções de análise ajustando o nível de análise. Arraste o cursor pela escala para definir o nível de análise pretendido. Utilize a descrição do lado direito da escala para escolher o nível de análise que melhor se adequa às suas necessidades.

      Os utilizadores avançados podem aproveitar as definições que o Bitdefender oferece. Para configurar as opções de análise em pormenor, clique em **Personalizar**. Pode encontrar informação sobre as mesmas no final desta secção.

   b. Também pode configurar as seguintes opções gerais:

      - **Executar a tarefa com prioridade baixa .** Diminui a prioridade do processo de análise. Irá permitir que outros programas funcionem com maior rapidez e aumenta o tempo necessário para terminar o processo da análise.
      - **Minimizar a janela da análise para a área de notificação .** Minimiza a janela da análise para a área de notificação. Faça duplo-clique sobre o ícone Bitdefender para o abrir.
      - Especifique a ação a aplicar se não forem encontradas ameaças.

   c. Clique em **OK** para guardar as alterações e fechar a janela.

6. Utilize o botão **Agendar** se pretender definir uma agenda para a sua tarefa de análise. Selecione uma das opções correspondentes para definir uma agenda:
   - No iniciar do sistema
   - Uma vez
   - Periodicamente
7. Selecione o tipo de análise que deseja executar na janela **Tarefa de análise**.
8. Clique em **Iniciar Análise** e siga o assistente de Análise Antivírus para completar a análise. Dependendo das localizações a serem analisadas, a análise pode demorar um pouco. No final da análise, será notificado para escolher as ações que devem ser tomadas nos ficheiros detetados, caso os haja.
9. Se quiser, pode voltar a executar rapidamente uma análise personalizada anterior ao clicar na entrada correspondente na lista disponível.

Informação sobre as opções de análise

Poderá achar esta informação útil:

- Se não está familiarizado com alguns dos termos, procure-os no glossário. Pode também encontrar informação útil pesquisando a Internet.
- **Análise de ficheiros.** Pode configurar o Bitdefender para analisar todos os tipos de ficheiros ou apenas aplicações (ficheiros de programas). A análise de todos os ficheiros proporciona uma maior segurança, enquanto a análise das aplicações só pode ser utilizada numa análise mais rápida.

  As aplicações (ou ficheiros de programa) são muito mais vulneráveis a ataques de malware do que qualquer outro tipo de ficheiros. Esta categoria inclui as seguintes extensões de ficheiro: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script;

sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Opções de análise para ficheiros.** Os arquivos que contém ficheiros infectados não são uma ameaça imediata à segurança do seu sistema. O malware só pode afetar o seu sistema se o ficheiro infectado for extraído do arquivo e executado sem que a proteção em tempo real esteja ativada. No entanto, é recomendado que utilize esta opção para detetar e remover qualquer ameaça potencial, mesmo se não for imediata.

  Nota
  Analisar ficheiros arquivados aumenta o tempo da análise e requer mais recursos do sistema.

- **Analisar sectores de arranque.** Pode definir o Bitdefenderpara analisar os sectores de saída do seu disco rígido. Este sector do disco rígido contém o código do computadores necessário para iniciar o processo de reinício. Quando um vírus infecta o sector de saída, a drive pode tornar-se inacessível ou poderá não conseguir iniciar o seu sistema e aceder aos seus dados.
- **Analisar Memória.** Selecione esta opção para analisar programas executados na memória do seu sistema.
- **Analisa registo.** Selecione esta opção para analisar as chaves de registo. O Registo do Windows é uma base de dados que armazena as definições da configuração e as opções para os componentes do sistema operativo Windows, bem como para as aplicações instaladas.
- **Analisa cookies.** Selecione esta opção para analisar os cookies armazenados pelos navegadores no seu computador.
- **Analisar só ficheiros alterados.** Ao analisar apenas ficheiros novos e modificados, pode melhorar significativamente o desempenho do seu sistema sem comprometer a sua segurança.
- **Ignorar keyloggers comerciais.** Selecione esta opção se tiver instalado e usar programas de controlo e registo comerciais no seu computador. Os programas de controlo e registo comerciais são software legítimo de monitorização do computador cuja função mais básica é registar tudo o que é digitado no teclado.

- **Analisar em busca de Rootkits.** Selecione esta opção para analisar rootkits e objetos ocultos usando tal software.

17.2.5. Assistente de Análise Antivírus

Sempre que inicie uma análise a-pedido (por exemplo, clicar botão direito sobre a pasta, apontar para o Bitdefender e selecionar **Analisar com Bitdefender**), o assistente de análise antivírus Bitdefender irá aparecer. Siga o assistente para concluir o processo de análise.

Nota

Se o assistente de análise não surgir, a análise poderá estar configurada para correr silenciosamente, em segundo plano. Procure pelo ícone do progresso da análise na área de notificação. Pode clicar nesse ícone para abrir a janela da análise e ver o seu progresso.

Passo 1 - Realizar Análise

Bitdefender iniciará a análise dos objetos selecionados. Pode ver informação em tempo real sobre o estado da análise e as estatísticas (incluindo o tempo decorrido, uma estimativa do tempo restante e o número de ameaças detetadas). Para ver mais detalhes, clique na hiperligação **Mostrar mais**.

Espere que o Bitdefender termine a análise. O processo de análise pode demorar algum tempo, dependendo da complexidade da mesma.

Parar ou pausar a análise. Pode interromper a análise a qualquer altura que quiser clicando em **Parar**. Irá directamente para o último passo do assistente. Para parar temporariamente o processo de análise, clique em **Pausa**. Terá de clicar em**Retomar** para retomar a análise.

Arquivos protegidos com palavra-passe. Quando é detetado um arquivo protegido por palavra-passe, dependendo das definições da análise, poderá ter de indicar a palavra-passe. Os arquivos protegidos por palavra-passe não podem ser analisados a não ser que forneça a palavra-passe. Estão disponíveis as seguintes opções:

- **Palavra-passe.** Se quer que o Bitdefender analise o arquivo, selecione esta opção e insira a palavra-passe. Se não sabe a palavra-passe, escolha uma das outras opções.
- **Não pergunte pela palavra-passe e não analise este objeto.** Selecione esta opção para saltar a análise deste arquivo.

- **Passar todos os itens protegidos por password sem os analisar.** Selecione esta opção se não deseja ser incomodado acerca de arquivos protegidos por palavra-passe. O Bitdefender não será capaz de os analisar, mas um registo dos mesmos será mantido no relatório da análise.

Escolha a opção desejada e clique em **OK** para continuar a analisar.

Passo 2 - Escolher Ações

No final da análise, será notificado para escolher as ações que devem ser tomadas nos ficheiros detetados, caso os haja.

Nota

Quando executa uma análise rápida ou uma análise completa ao sistema, o Bitdefender toma automaticamente as ações recomendadas nos ficheiros detetados durante a análise. Se ainda houver ameaças não resolvidas, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas.

Os objetos infectados são apresentados em grupos, baseados no tipo de malware com que estão infectados. Clique no link correspondente a uma ameaça para descobrir mais informação acerca dos objetos infectados.

Pode escolher uma ação geral a ser levada a cabo para todas as incidências ou pode escolher ações separadas para cada grupo de incidências. Uma ou várias das seguintes opções poderão aparecer no menu:

Tomar ações adequadas

Bitdefender tomará as ações recomendadas dependendo do tipo de ficheiro detetado:

- **Ficheiros infectados.** Os ficheiros detetados como infectados correspondem a uma assinatura de malware na Base de Dados de Assinaturas de Malware do Bitdefender. Bitdefender tentará automaticamente remover o código malware do ficheiro infetado e reconstruir o ficheiro original. Esta operação é designada por desinfecção.

  Os ficheiros que não podem ser desinfectados são movidos para a quarentena de modo a conter a infecção. O ficheiros em quarentena não podem ser executados ou abertos; logo o risco de infectarem o seu computador desaparece. Para mais informação, por favor consulte o "*Gerir ficheiros da quarentena*" (p. 107).

Importante
Para determinados tipos de malware, a desinfecção não é possível por o ficheiro detectado ser totalmente malicioso. Nestes casos, o ficheiro infectado é eliminado do disco.

- **Ficheiros suspeitos.** Os ficheiros são detetados como suspeitos pela análise heurística. Não foi possível desinfectar os ficheiros suspeitos por não estar disponível uma rotina de desinfecção. Serão movidos para a quarentena para evitar uma potencial infeção.

  Por defeito, os ficheiros da quarentena são automaticamente enviados para os Laboratórios Bitdefender para serem analisados pelos investigadores de malware da Bitdefender. Se a presença de malware for confirmada, é emitida uma assinatura para possibilitar a remoção do malware.

- **Aquivos que contêm ficheiros infetados.**
  - Os arquivos que contêm apenas ficheiros infetados são eliminados automaticamente.
  - Se um arquivo tiver ficheiros infectados e limpos, o Bitdefender tentará eliminar os ficheiros infectados desde que possa reconstruir o arquivo com os ficheiros limpos. Se não for possível a reconstrução do arquivo, será informado de que não pode ser tomada qualquer ação, de forma a evitar perder ficheiros limpos.

Apagar
Remove os ficheiros detetados do disco.

Se os ficheiros infectados estiverem armazenados num arquivo junto com ficheiros limpos, o Bitdefender tentará eliminar os ficheiros infectados e reconstruir o arquivo com ficheiros limpos. Se não for possível a reconstrução do arquivo, será informado de que não pode ser tomada qualquer ação, de forma a evitar perder ficheiros limpos.

Não Tomar Ação
Nenhuma ação será levada a cabo sobre os ficheiros detetados. Após a analisar terminar, pode abrir o relatório da análise para ver informação sobres esses ficheiros.

Clique em **Continuar** para aplicar as ações especificadas.

Passo 3 - Resumo

Quando o Bitdefender termina de reparar estas incidências, o resultado da análise aparecerá numa nova janela. Se deseja uma informação completa sobre o processo de análise, clique em **Mostrar Relatório** para ver o relatório da análise.

Clique em **Fechar** para fechar a janela.

Importante

Na maioria dos casos o Bitdefender desinfecta com sucesso o ficheiro infectado ou isola a infecção. No entanto, há incidências que não puderam ser automaticamente resolvidas. Se necessário, ser-lhe-á solicitado que reinicie o seu computador, para que o processo de limpeza seja completado. Para mais informações e instruções sobre como remover manualmente o malware, por favor consulte "*Remover malware do seu sistema*" (p. 215).

17.2.6. Ver os relatórios da análise

Sempre que uma análise for efetuada, é criado um registo de análise e o Bitdefender regista as incidências detectadas na janela Antivírus. O relatório da análise contém informação detalhada acerca dos processos de análise registados, tal como as opções da análise, o alvo da análise, as ameaças encontradas e as ações tomadas sobre essas ameaças.

Pode abrir o relatório diretamente no assistente de análise, assim que esta terminar, clicando em **Mostrar Relatório**.

Para analisar mais tarde um relatório de análise ou qualquer infeção detetada, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no ícone na parte superior da janela e selecione **Definições Gerais** do menu suspenso.
3. Na janela **Eventos**, selecione **Antivírus** do menu suspenso correspondente.

   Aqui poderá encontrar todos os eventos de análise malware, incluindo ameaças detetadas na análise no acesso, análises iniciadas pelo utilizador e alterações de estado para as análises automáticas.
4. Na lista de eventos, pode ver as análises que foram recentemente efetuadas. Clique no evento para visualizar detalhes sobre o mesmo.
5. Para abrir o relatório da análise, clique em **Ver Relatório**.

17.3. Análise automática de média removíveis

O Bitdefender deteta automaticamente quando um dispositivo de armazenamento removível se liga ao computador e analisa-o em segundo plano. Isto é recomendado para prevenir que virus e malware infectem o seu computador.

Os dispositivos detetados encaixam-se numa destas categorias:

- CDs/DVDs
- Dispositivos de armazenamento USB, tais como pens e discos rígidos externos
- Unidades de Rede Mapeadas (remotas)

Você pode configurar a análise automática separadamente para cada categoria de dispositivos de armazenamento. Análise automática das drives de rede mapeadas está desativada por defeito.

17.3.1. Como funciona?

Quando deteta dispositivos de armazenamento removíveis, o Bitdefender começa a verificar se existe malware em segundo plano (desde que a análise automática esteja ativada para aquele tipo de dispositivo). Um ícone de análise do Bitdefender irá aparecer no tabuleiro do sistema Pode clicar nesse ícone para abrir a janela da análise e ver o seu progresso.

Se o Piloto Automático estiver ativado, não será incomodado com a análise. A análise será apenas registada e a informação sobre a mesma ficará disponível na janela Eventos.

Se o Piloto Automático estiver desativado:

1. Será notificado através de uma janela de pop-up que um novo dispositivo foi detetado e está a ser analisado.
2. Na maioria dos casos, o Bitdefender remove automaticamente o malware detetado ou isola os ficheiros infectados na quarentena. Se houver ameaças não resolvidas depois da análise, ser-lhe-á solicitado que escolha as ações a tomar perante as mesmas.

> **Nota**
> Leve em consideração que não pode ser tomada qualquer acção em ficheiros infectados ou suspeitos detectados em CDs/DVDs. Da mesma forma, não pode ser tomada qualquer acção em ficheiros infectados ou

suspeitos detectados em drives de rede mapeadas, caso não tenha os privilégios adequados.

3. Quando a análise estiver concluída, é apresentada a janela dos resultados da análise para o informar se pode aceder em segurança aos ficheiros nos dispositivos removíveis.

Esta informação pode ser útil para si:

- Por favor tenha cuidado ao usar um CD/DVD infectado com malware, porque o malware não pode ser removido do disco (é apenas de leitura). Certifique-se que a proteção em tempo real está ativada para evitar que o malware se propague no seu sistema. Será melhor copiar os dados mais importantes do disco para o seu sistema e depois eliminá-los do disco.
- Em alguns casos, o Bitdefender poderá não conseguir remover o malware de ficheiros específicos devido a restrições legais ou técnicas. Exemplo disso são os ficheiros guardados usando uma tecnologia proprietária (isto acontece porque o ficheiro não pode ser correctamente recriado).

  Para saber como lidar com malware, por favor consulte "*Remover malware do seu sistema*" (p. 215).

17.3.2. Gerir análise de média removível

Para gerir a análise automática dos média removíveis, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Antivírus**.
4. Na janela **Antivírus**, selecione o separador **Exceções**.

Para uma melhor proteção, recomenda-se que ligue a análise automática para todos os tipos de dispositivos de armazenamento removíveis.

As opções de análise estão pré-configuradas para obter os melhores resultados de deteção. Se forem detectados ficheiros infectados, o Bitdefender tentará desinfectá-los (remover o código malware) ou movê-los para a quarentena. Se ambas as acções falharem, o assistente da Análise Antivírus permite especificar outras acções a serem tomadas com ficheiros infectados. As opções de análise são padronizadas e não as pode alterar.

17.4. Configurar exceções da análise

O Bitdefender permite excluir ficheiros, pastas ou extensões de ficheiros específicos da análise. Esta característica visa evitar a interferência com o seu trabalho e também pode ajudar a melhorar o desempenho do sistema. As exceções devem ser usadas por utilizadores com conhecimentos informáticos avançados ou sob as recomendações de um representante da Bitdefender.

Pode configurar as exceções para aplicar apenas na análise no acesso ou a pedido, ou ambos. Os objetos excluídos da análise a-pedido não serão analisados, independentemente de eles serem acedidos por si ou por uma aplicação.

Nota

As exceções NÃO serão aplicadas à análise contextual. Análise Contextual é um tipo de análise a-pedido: você clica com o botão direito de rato sobre o ficheiro ou pasta que quer analisar e seleciona **Analisar com Bitdefender**.

17.4.1. Excluir pastas e ficheiros da análise

Para excluir ficheiros ou pastas específicas da análise, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Antivírus**.
4. Na janela **Antivírus**, selecione o separador **Exceções**.
5. Ative as exceções para os ficheiros que utilizem o respetivo botão.
6. Clique na ligação **Ficheiros e pastas excluídos**. Na janela que surge, pode gerir os ficheiros e pastas excluídos da análise.
7. Adicionar exceções seguindo estes passos:
   a. Clique no botão **Adicionar** , localizado no cimo da tabela de exceções.
   b. Clique em **Explorar**, selecione o ficheiro ou pasta que deseja excluir da análise e depois clique **OK**. Alternativamente, pode digitar (ou copiar e colar) o caminho para o ficheiro ou pasta no campo editar.

c. Por defeito, o ficheiro ou pasta é excluída da análise no acesso e a pedido. Para alterar a aplicação da exclusão, selecione uma das outras opções.

d. Prima **Adicionar**.

8. Clique em **OK** para guardar as alterações e fechar a janela.

17.4.2. Excluir extensões de ficheiros da análise

Quando exclui uma extensão de ficheiro da análise, o Bitdefender deixará de analisar ficheiros com essa extensão, independentemente da sua localização no seu computador. A exclusão também se aplica a ficheiros em média removíveis, tais como CDs, DVDs, dispositivos de armazenamento USB ou drives da rede.

Importante
Tenha cuidado ao excluir as extensões da análise, porque tais exceções podem tornar o seu computador vulnerável ao malware.

Para excluir extensões de ficheiros da análise, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Antivírus**.
4. Na janela **Antivírus**, selecione o separador **Exceções**.
5. Ative as exceções para os ficheiros que utilizem o respetivo botão.
6. Clique na ligação **Extensões excluídas**. Na janela que surge, pode gerir as extensões de ficheiros excluídas da análise.
7. Adicionar exceções seguindo estes passos:
   a. Clique no botão **Adicionar** , localizado no cimo da tabela de exceções.
   b. Introduza as extensões que deseja excluir da análise, separando-as com ponto e vírgula (;). Eis um exemplo:

      txt;avi;jpg

   c. Por defeito, todos os ficheiros com as extensões especificadas são excluídas na análise no acesso e a pedido. Para alterar a aplicação da exclusão, selecione uma das outras opções.
   d. Prima **Adicionar**.

8. Clique em **OK** para guardar as alterações e fechar a janela.

17.4.3. Gerir exceções da análise

Se as exceções de análise configuradas já não forem necessárias, recomenda-se que elimine ou desative as exceções da análise.

Para gerir as exceções da análise, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Antivírus**.
4. Na janela **Antivírus**, selecione o separador **Exceções**. Use a opções na secção **Ficheiros e pastas** para gerir as exceções de análise.
5. Para remover ou editar exceções da análise, clique numa das ligações disponíveis. Proceder da seguinte forma:
   - Para eliminar um item da lista, selecione-o e clique no botão **Remover**.
   - Para editar uma entrada da lista, clique duas vezes (ou selecione-a e clique no botão **Editar**). Aparecerá uma nova janela onde poderá alterar a extensão ou o caminho a ser excluído e o tipo de análise da qual quer que eles sejam excluídos. Faça as alterações necessárias, depois clique em **Modificar**.
6. Para desativar exceções da análise, utilize o respetivo botão.

17.5. Gerir ficheiros da quarentena

O Bitdefender isola os ficheiros infectados com malware que não consegue desinfectar numa área segura denominada quarentena. Quando o vírus se encontra na quarentena não pode provocar nenhum mal, porque não pode ser nem lido nem executado.

Por defeito, os ficheiros da quarentena são automaticamente enviados para os Laboratórios Bitdefender para serem analisados pelos investigadores de malware da Bitdefender. Se a presença de malware for confirmada, é emitida uma assinatura para possibilitar a remoção do malware.

Além disso, o Bitdefender analisa os ficheiros em quarentena após cada atualização das assinaturas de malware. Os ficheiros limpos são automaticamente repostos no seu local de origem.

Para verificar e gerir ficheiros da quarentena, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Antivírus**.
4. Na janela **Antivírus**, selecione o separador **Quarentena**.
5. Os ficheiros da quarentena são geridos automaticamente pelo Bitdefender de acordo com as predefinições da quarentena. Embora não seja recomendado, pode ajustar as definições da quarentena de acordo com as suas preferências.

   Analisar quarentena após nova atualização
   Mantenha esta opção ligada para analisar automaticamente os ficheiros da quarentena após cada atualização das definições de vírus. Os ficheiros limpos são automaticamente repostos no seu local de origem.

   Enviar ficheiros suspeitos da quarentena para posterior análise
   Mantenha esta opção ligada para enviar automaticamente os ficheiros da quarentena para os Laboratórios da Bitdefender. As amostras de ficheiros serão analisados pelos investigadores de malware da Bitdefender. Se a presença de malware for confirmada, é emitida uma assinatura para possibilitar a remoção do malware.

   Apagar conteúdo com mais de {30} dias
   Por defeito, os ficheiros da quarentena com mais de 30 dias são automaticamente eliminados. Se quiser alterar este intervalo, digite um novo valor no campo correspondente. Para desativar a eliminação automática dos antigos ficheiros da quarentena, tipo 0.
6. Para eliminar um ficheiro da quarentena, selecione-o e clique no botão **Eliminar**. Se pretende restaurar um ficheiro da quarentena para a respetiva localização original, selecione-o e clique em **Restaurar**.

17.6. Controlo Ativo de Vírus

O Controlo Ativo de Vírus da Bitdefender é uma tecnologia de deteção proativa inovadora que usa métodos heurísticos para detetar novas e potenciais ameaças em tempo real.

O Controlo de Vírus Activo monitoriza as aplicações executados no computador, procurando acções identificáveis como malware. Cada uma

destas acções é classificada e é calculada uma pontuação geral para cada processo. Quando a classiificação geral para um processo atinge um dado limite, o processo é considerado perigoso e é bloqueado automaticamente.

Se o Piloto Automático estiver desativado, será notificado através de uma janela de pop-up acerca da aplicação bloqueada. Caso contrário, a aplicação será bloqueada sem qualquer notificação. Pode verificar que aplicações foram detetadas pelo Controlo Ativo de Vírus na janela Eventos.

17.6.1. Verificar aplicações detetadas

Para verificar as aplicações detetadas pelo Controlo Ativo de Vírus, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Clique no ícone na parte superior da janela e selecione **Definições Gerais** do menu suspenso.
3. Na janela **Eventos**, selecione **Antivírus** do menu suspenso correspondente.
4. Clique no evento para visualizar detalhes sobre o mesmo.
5. Se confiar na aplicação, pode configurar o Controlo Ativo de Vírus para não a bloquear, clicando em **Permitir e monitorizar**. O Controlo Activo de Vírus continuará a monitorizar as aplicações excluídas. Se uma aplicação excluída for detectada a realizar actividades suspeitas, o evento será simplesmente registado e comunicado à Nuvem do Bitdefender como uma detecção de erro.

17.6.2. Ligar ou desligar o Controlo Ativo de Vírus

Para ativar ou desativar o Controlo Ativo de Vírus, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Antivírus**.
4. Na janela **Antivírus**, selecione o separador **Escudo**.
5. Clique no botão para ativar ou desativar o Controlo Ativo de Vírus.

17.6.3. Ajustar proteção de Controlo de Vírus Ativo

Se verifica que o Controlo Ativo de Vírus deteta frequentemente aplicações legítimas, deve definir um nível de proteção inferior.

Para ajustar a proteção do Controlo Ativo de Vírus , siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Antivírus**.
4. Na janela **Antivírus**, selecione o separador **Escudo**.
5. Assegure-se que o Controlo Ativo de Vírus está ligado.
6. Arraste o cursor pela escala para definir o nível de proteção pretendido. Utilize a descrição do lado direito da escala para escolher o nível de proteção que melhor se adequa às suas necessidades de segurança.

> **Nota**
> Quando define um nível de protecção superior, o Controlo Activo de Vírus irá requerer menos sinais de comportamento malware para comunicar um processo. Isto provocará um aumento do número de aplicações que são comunicadas e, ao mesmo tempo, a um aumento da probabilidade de falsos positivos (aplicações limpas detectadas como maliciosas).

17.6.4. Gerir processos excluídos

Pode configurar as regras de exclusão para aplicações de confiança para que o Controlo Ativo de Vírus não as bloqueie, se realizarem ações como as do malware. O Controlo Activo de Vírus continuará a monitorizar as aplicações excluídas. Se uma aplicação excluída for detectada a realizar actividades suspeitas, o evento será simplesmente registado e comunicado à Nuvem do Bitdefender como uma detecção de erro.

Para gerir o processo de exceções do Controlo Ativo de Vírus, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Antivírus**.
4. Na janela **Antivírus**, selecione o separador **Exceções**.

5. Clique na hiperligação **Processos Excluídos**. Na janela que aparece, pode gerir as exceções do processo de Controlo Ativo de Vírus.

   Nota
   As exclusões do processo também aplicam-se a Deteção de Invasão.

6. Adicionar exceções seguindo estes passos:
   a. Clique no botão **Adicionar** , localizado no cimo da tabela de exceções.
   b. Clique em **Explorar**, procure e selecione a aplicação que quer excluir e depois clique em **OK**.
   c. Manter a opção **Permitir** selecionada para evitar que o Controlo Ativo de Vírus bloqueie a aplicação.
   d. Prima **Adicionar**.
7. Para remover ou editar exceções, proceda da seguinte forma:
   - Para eliminar um item da lista, selecione-o e clique no botão **Apagar**.
   - Para editar uma entrada da lista, clique duas vezes (ou selecione-a) e clique no botão **Modificar**. Faça as alterações necessárias, depois clique em **Modificar**.
8. Guardar as alterações e fechar a janela.

18. ANTISPAM

Spam é o termo utilizado para descrever mensagens eletrónicas não solicitadas. O Spam é um problema crescente, tanto para indíviduos como para organizações. Não é bonito, não desejaria que os seus filhos o vissem, pode fazer com que seja despedido (por desperdiçar muito tempo, ou por receber pornografia no seu mail de trabalho) e não pode impedir que as pessoas o enviem. O melhor a fazer para impedir isso, é, obviamente, parar de o receber. Infelizmente, o Spam vem em muitos formatos e feitios, e é muito abundante.

O Bitdefender Antispam emprega inovações tecnológicas surpreendentes e um conjunto de filtros de antispam standard para limpar o spam antes de o mesmo chegar à caixa de correio A receber do utilizador. Para mais informação, por favor consulte o "*Compreender o Antispam*" (p. 113).

A proteção de Antispam do Bitdefender está disponível apenas para clientes de correio eletrónico configurado para receber mensagens de e-mail via protocolo POP3. POP3 é um dos protocolos mais utilizados para fazer o download de mensagens de e-mail a partir de um servidor de correio.

Nota
O Bitdefender não proporciona proteção antispam para contas de correio eletrónico a que acede através de sites Internet (webmail).

As mensagens não solicitadas detetadas pelo Bitdefender são marcadas com o prefixo [SPAM] no campo do assunto. O Bitdefender move automaticamente as mensagens de spam para uma determinada pasta, da seguinte forma:

- No Microsoft Outlook, as mensagens de spam são movidas para a pasta **Spam**, localizada na pasta **Itens Eliminados**. A pasta **Spam** é criada durante a instalação do Bitdefender.
- No Outlook Express e no Windows Mail, as mensagens de spam são movidas diretamente para os **Itens Eliminados**.
- No Mozilla Thunderbird, as mensagens de spam são movidas para a pasta **Spam**, localizada na pasta **Lixo**. A pasta **Spam** é criada durante a instalação do Bitdefender.

Se usa outros cliente de e-mail, tem de criar uma regra para mover os e-mails marcados como [spam] pelo Bitdefender para uma pasta de quarentena personalizada.

18.1. Compreender o Antispam

18.1.1. Filtros impeditivos da entrada de mails indesejados

O Motor Antispam do Bitdefender inclui proteção na nuvem e outros filtros diferenciados que garantem que a sua Caixa de Entrada fique livre de SPAM, como a Lista de Amigos, Lista de Spammers e Filtro de Carateres.

Lista de Amigos / Lista de Spammers

A maioria das pessoas comunica regularmente com um grupo de pessoas, ou até mesmo recebe mensagens de empresas ou organizações no mesmo domínio. Ao utilizar as **listas de amigos ou spammers**, pode facilmente decidir de quem pretende receber e-mails (amigos) independentemente do conteúdo das mensagens, ou de quem nem sequer pretende ouvir falar novamente (spammers).

Nota
Recomendamos que adicone os nomes e endereços de e-mail dos seus amigos à **Lista de Amigos**. O Bitdefendernão bloqueia mensagens das pessoas dessa lista; logo, adicionar amigos ajuda a que as mensagens legítimas cheguem a si.

Filtro caracteres

Muitas mensagens de spam estão escritas em Cirílico e/ou caracteres Asiáticos. O filtro de Caracteres detecta este tipo de mensagens e marca-os como SPAM.

18.1.2. Operação Antispam

O Motor Bitdefender Antispam usa todos os filtros antispam combinados para determinar se um determinado e-mail deve de chegar à pasta **A Receber** ou não.

Todo o e-mail proveniente da Internet é inicialmente verificado pelo filtro da Lista Amigos / Lista Spammers. Se o endereço do remetente se encontrar na Lista Amigos, o e-mail é movido directamente para a sua **Caixa de Entrada**.

Caso contrário, o filtro da Lista de Spammers irá apoderar-se do seu correio electrónico para verificar se o endereço do remetente se encontra na lista. Se for encontrada uma correspondência, a mensagem será marcada como SPAM e movida para a pasta de **Spam**.

Ainda, o Filtro caracteres irá verificar se o e-mail está escrito em caracteres Cirílicos ou Asiáticos. Se assim for, e-mail será marcado com Indesejado e movido para a pasta de **Spam**.

> **Nota**
> Se o e-mail for marcado com SEXUALLY EXPLICIT na linha do sujeito, o Bitdefender irá considerá-lo como SPAM.

18.1.3. Clientes de email e protocolos suportados

A proteção Antispam é fornecida para todos os clientes de e-mail POP3/SMTP. No entanto a barra de ferramentas do Antispam Bitdefender apenas se integra em:

- Microsoft Outlook 2007 / 2010 / 2013
- Microsoft Outlook Express e Windows Mail (em sistemas de 32 bits)
- Mozilla Thunderbird 3.0.4

18.2. Ligar ou desligar a proteção antispam

A proteção AntiSpam está ativada por defeito.

Para desativar o módulo de AntiSpam, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Antispam**.
4. Na janela **Antispam**, clique no botão para ativar ou desativar o **Antispam**.

18.3. Utilizar a barra de ferramentas Antispam na janela do seu cliente de email

No lado superior da janela do seu cliente de mail pode ver a barra de ferramentas do Antispam. A barra de ferramentas do Antispam ajuda-o a gerir a proteção antispam diretamente do seu cliente de e-mail. Pode facilmente corrigir o Bitdefender se ele marcar uma mensagem legítima como SPAM.

Importante

O BiDefender integra uma barra antispam de facil utilização, nos clientes de email mais comuns. Para ver a lista completa de clientes de e-mail suportados, por favor consulte o "*Clientes de email e protocolos suportados*" (p. 114).

Cada botão é explicado abaixo:

É Spam - indica que o email selecionado é spam. O email será movido imediatamente para a pasta **Spam**. Se os serviços da nuvem antispam estiverem ativados, a mensagem é enviada para a Nuvem do Bitdefender para análise mais aprofundada.
Não Spam - indica que o email selecionado não é spam e o Bitdefender não o deveria ter identificado. Este e-mail será movido da pasta **Spam** para o diretório **Caixa de Entrada**. Se os serviços da nuvem antispam estiverem ativados, a mensagem é enviada para a Nuvem do Bitdefender para análise mais aprofundada.

Importante

O botão **Não Spam** fica ativo quando selecionar uma mensagem marcada como SPAM pelo Bitdefender (normalmente estas mensagens localizam-se na pasta de **Spam**).

Adicionar Spammer - adiciona o remetente da mensagem de e-mail à lista de Spammers. Pode necessitar de clicar em **OK** para confirmar. As mensagens de e-mail recebidas dos endereços na lista de Spammers são automaticamente marcadas como [spam].
Adicionar Amigo - adiciona o remetente da mensagem de e-mail à lista de Amigos. Pode necessitar de clicar em **OK** para confirmar. Irá sempre receber mensagens de e-mail destes endereços, independentemente do conteúdo da mensagem.
Spammers- abre a **Lista de Spammers** que contém todos os endereços de e-mail, dos quais não quer receber mensagens, independentemente do seu conteúdo. Para mais informação, por favor consulte o "*Configurar a lista de Spammers*" (p. 118).
Amigos - abre a **Lista de amigos** que contém todos os endereços de e-mail dos quais deseja receber mensagens de e-mail, independentemente do seu conteúdo. Para mais informação, por favor consulte o "*Configurar a Lista de Amigos*" (p. 117).
Definições - abre uma janela onde pode configurar as definições da barra de ferramentas e dos filtros antispam.

18.3.1. Indicar os erros de deteção

Se estiver a usar um cliente de e-mail suportado, pode facilmente corrigir o filtro antispam (indicando mensagens de correio eletrónico que não deveriam ter sido marcadas como[spam]). Se o fizer, ajuda a melhorar a eficiência do filtro antispam. Siga os seguintes passos:

1. Abra o mail de cliente.
2. Vá à pasta de lixo eletrónico, para onde são movidas as mensagens.
3. Selecione a mensagem legítima incorretamente marcada como [spam] pelo Bitdefender.
4. Clique no botão **Adicionar Amigos** da barra de tarefas antispam do Bitdefender para adicionar o remetente à lista de Amigos. Pode necessitar de clicar em **OK** para confirmar. Irá sempre receber mensagens de e-mail destes endereços, independentemente do conteúdo da mensagem.
5. Clique no botão **Não Spam** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela de mail do cliente). A mensagem de email será movida para a pasta de Entrada.

18.3.2. Indicar mensagens de spam não detetadas

Se estiver a utilizar um cliente de e-mail suportado, pode facilmente indicar quais as mensagens de e-mail que devem ser detectadas como spam. Se o fizer, ajuda a melhorar a eficiência do filtro antispam. Siga os seguintes passos:

1. Abra o mail de cliente.
2. Vá à pasta Caixa de Entrada.
3. Selecione as mensagens spam não detetadas
4. Clique no botão **É Spam** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela de email do cliente). São imediatamente marcadas como [spam] e movidas para a pasta de lixo electrónico.

18.3.3. Configurar definições da barra de ferramentas

Para configurar as definições da barra de ferramentas antispam do seu cliente de email, clique no botão **Definições** na barra e depois no separador **Definições da Barra de Ferramentas**.

Tem as seguintes opções:

- **Mova a mensagem para os Itens Eliminados** (apenas para o Microsoft Outlook Express / Windows Mail)

  Nota
  No Microsoft Outlook / Mozilla Thunderbird, as mensagens de spam são automaticamente movidas para uma pasta de Spam, localizada nos Itens Eliminados / Pasta Lixo.

- **Marque as mensagens de e-mail indesejadas como 'ler'** - marca as mensagens indesejadas como ler automaticamente, para que não seja perturbador quando chegarem.
- Pode optar por visualizar janelas de confirmação quando clica nos botões **Adicionar Spammer** e **Adicionar Amigo** na barra de ferramentas antispam.

  As janelas de confirmação pode evitar a adição acidental de destinatários de email à lista de Amigos / Spammers.

18.4. Configurar a Lista de Amigos

A **Lista de Amigos** é uma lista de todos os endereços de e-mail dos quais deseja sempre receber mensagens, independentemente do seu conteúdo. As mensagens dos seus amigos não são marcadas como spam, mesmo que o conteúdo se assemelhe a spam.

Nota
Qualquer mail proveniente de um endereço presente na **Lista de amigos**, será automaticamente entregue na sua Caixa de Entrada, sem mais demora.

Para configurar e gerir a lista de Amigos:

- Se estiver a utilizar o Microsoft Outlook/Outlook Express/Windows Mail/Thunderbird, clique no botão **Amigos** na barra de ferramentas antispam do Bitdefender.
- Em alternativa, proceda da seguinte forma:
  1. Abra a janela de Bitdefender.
  2. Aceda ao painel de **Proteção**.
  3. No módulo **Antispam**, selecione **Gerir Amigos**.

Para adicionar um endereço de email, selecione a opção **Endereço de email**, digite o endereço e depois clique em **Adicionar**. Sintaxe: nome@dominio.com.

Para adicionar os endereços eletrónicos de um domínio específico, selecione a opção **Nome do domínio**, insira o nome do domínio e depois clique em **Adicionar**. Sintaxe:

- @dominio.com, *dominio.com e dominio.com - todos os mails provenientes de dominio.com chegarão à sua **Caixa de Entrada** independentemente do seu conteúdo;
- *dominio* - todos os mails provenientes de dominio (sem interessar os sufixos do dominio) chegarão à sua **Caixa de Entrada** independentemente do seu conteúdo;
- *com - todos os mails que têm este sufixo de domínio com chegarão à sua **Caixa de Entrada** independentemente do seu conteúdo.

É recomendado que evite adicionar domínios completos, mas isto poderá ser útil em algumas situações. Por exemplo, pode adicionar o domínio do endereço eletrónico da empresa para a qual trabalha ou de parceiros de confiança.

Para eliminar um item da lista, clique na ligação **Remover** correspondente. Para eliminar todas as entradas da lista, clique no botão **Limpar Lista**.

Pode guardar a lista de Amigos num ficheiro para que mais tarde possa usá-lo noutro computador ou quando reinstalar o produto. Para guarda a lista de Amigos, clique no botão **Guardar** e guarda no local desejado. O ficheiro terá a extensão .bwl

Para carregar uma lista de Amigos previamente guardada, clique no botão **Carregar** e abra o ficheiro .bwl correspondente. Para repor o conteúdo da lista existente ao carregar uma lista guardada anteriormente, selecione **Sobrescrever lista atual**.

Clique em **OK** para guardar as alterações e fechar a janela.

18.5. Configurar a lista de Spammers

A **Lista de indesejados** é uma lista de todos os endereços de e-mail, dos quais nunca pretende receber mensagens, independentemente do seu conteúdo. Todo o mail proveniente de um endereço presente na **Lista de indesejados**, será marcado automaticamente com indesejado, sem mais demora.

Para configurar e gerir a lista de Spammers:

- Se estiver a utilizar o Microsoft Outlook/Outlook Express/Windows Mail/Thunderbird, clique no botão **Spammers** na barra de ferramentas antispam do Bitdefender integrada no seu cliente de e-mail.
- Em alternativa, proceda da seguinte forma:
  1. Abra a janela de Bitdefender.
  2. Aceda ao painel de **Proteção**.
  3. No módulo **Antispam**, selecione **Gerir Spammers**.

Para adicionar um endereço de email, selecione a opção **Endereço de email**, digite o endereço e depois clique em **Adicionar**. Sintaxe: nome@dominio.com.

Para adicionar os endereços eletrónicos de um domínio específico, selecione a opção **Nome do domínio**, insira o nome do domínio e depois clique em **Adicionar**. Sintaxe:

- @dominio.com, *dominio.com e dominio.com - todos os mails provenientes de dominio.com serão marcados como INDESEJADOS;
- *dominio* - todos os mails provenientes de dominio (independentemente dos sufixos de domínio) serão marcados como INDESEJADOS;
- *com - todos os mails tendo o sufixo de domínio com serão marcados como INDESEJADOS.

É recomendado que evite adicionar domínios completos, mas isto poderá ser útil em algumas situações.

Atenção

Não adicione domínios de serviços web-mail (tais como o Yahoo, Gmail, Hotmail ou outro) à lista de Spammers. Caso contrário, as mensagens de email recebidas de algum utilizador registado nesses serviços será detectado como spam. Se, por exemplo, adicionar yahoo.com à lista de Spammer, todos as mensagens de e-mais recebidas do endereço yahoo.com, serão marcadas como [spam].

Para eliminar um item da lista, clique na ligação **Remover** correspondente. Para eliminar todas as entradas da lista, clique no botão **Limpar Lista**.

Pode guardar a lista de Spam num ficheiro para que mais tarde possa usá-lo noutro computador ou quando reinstalar o produto. Para guarda a lista de Spam, clique no botão **Guardar** e guarda no local desejado. O ficheiro terá a extensão .bwl

Para carregar uma lista de spammers previamente guardada, clique no botão **Carregar** e abra o ficheiro .bwl correspondente. Para repor o conteúdo da

lista existente ao carregar uma lista guardada anteriormente, selecione **Sobrescrever lista atual**.

Clique em **OK** para guardar as alterações e fechar a janela.

18.6. A configurar os filtros locais Antispam

Como descrito em "*Compreender o Antispam*" (p. 113), o Bitdefender utiliza um conjunto de diferentes filtros antispam para identificar o spam. Os filtros antispam são pré-configurados para uma proteção eficaz.

> **Importante**
>
> Dependendo se recebe ou não mensagens eletrónicas fiáveis ou não escrita com caracteres asiáticos ou cirílicos, desative ou ative a definição que bloqueia automaticamente estas mensagens. A respetiva definição está desativada nas versões localizadas do programa que utilizam conjuntos de caracteres (por exemplo, na versão russa ou chinesa).

Para configurar os filtros locais antispam, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Antispam**.
4. Na janela **Antispam**, selecione o separador **Definições**.
5. Clique nos botões para ativar ou desativar os filtros locais antispam.

Se estiver a usar Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, pode configurar os filtros locais antispam diretamente a partir do seu cliente de email. Clique no botão **Definições** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela de mail do cliente) e depois no separador **Filtros Antispam**.

18.7. Configurar as definições da nuvem

A deteção na nuvem utiliza os Serviços na Nuvem do Bitdefender para lhe proporcionar uma proteção antispam eficaz e sempre atualizada.

As funções de proteção na nuvem enquanto mantiver o AntiSpam do Bitdefender ativado.

As amostras de emails legítimos ou spam podem ser enviados para a Nuvem Bitdefender quando indica erros de detecção ou emails de spam não detectados. Isto ajuda a melhorar a detecção antispam do Bitdefender.

Configurar o envio de amostra por e-mail para a Nuvem Bitdefender através da seleção das opções pretendidas, seguindo estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Antispam**.
4. Na janela **Antispam**, selecione as opções desejadas no separador **Definições**.

Se estiver a utilizar Microsoft Outlook/Outlook Express/Windows Mail/Thunderbird, pode configurar a deteção na nuvem diretamente a partir do seu cliente de e-mail. Clique no botão **Definições** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela de mail do cliente) e depois no separador **Definições de Nuvem**.

19. PROTEÇÃO DA INTERNET

A Proteção da Internet do Bitdefender garante uma experiência de navegação segura, alertando-o sobre possíveis páginas de phishing.

O Bitdefender fornece proteção da Internet em tempo real para:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari

Para configurar as definições de Proteção da Internet, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Proteção da Internet**.

Clique nos botões para ligar ou desligar:

- A mostrar a barra de ferramentas Bitdefender no navegador web.

> **Nota**
> A barra de ferramentas do browser do Bitdefender não está ativada por defeito.

- Consultor de pesquisa, um componente que qualifica os resultados do seu motor de pesquisa e dos links colocados nos websites das redes sociais ao colocar um icone ao lado de cada resultado:

  Não deveria visitar esta página web.

  Esta página web pode conter conteúdo perigoso. Tenha cuidado se decidir visitá-la.

  Esta página é segura.

  O Consultor de Pesquisa qualifica os resultados da pesquisa dos seguintes motores de busca:
  - Google
  - Yahoo!
  - Bing
  - Baidu

O Consultor de Pesquisa classifica os links publicados nos seguintes serviços das redes sociais:
- Facebook
- Twitter

- Analisar tráfego web SSL.

  Ataques mais sofisticados podem usar tráfego da web seguro para enganar as suas vítimas. É, por isso, recomendado que ative a análise SSL.

- Proteção contra fraudes.

- Proteção contra phishing.

Pode criar uma lista de páginas que não serão analisadas pelos motores antimalware, antiphishing e antifraude do Bitdefender. A lista deve conter apenas os sites web em que confia plenamente. Por exemplo, adicione os websites onde costuma frequentemente fazer compras on-line.

Para configurar e gerir páginas Web utilizando a proteção da Internet fornecida pelo Bitdefender, clique no link **Lista Branca**. Uma nova janela irá aparecer.

Para adicionar um site à lista branca, insira o seu endereço no campo correspondente e depois clique em **Adicionar**.

Para remover um site web desta lista, selecione-o na lista e clique na hiperligação **Remover** correspondente.

Clique em **Guardar** para guardar as alterações e fechar a janela.

19.1. Proteção do Bitdefender no navegador da web

Bitdefender integra-se diretamente através de uma barra de tarefas intuitiva e fácil de usar nos seguintes exploradores da Internet:

- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Safari

A barra de ferramentas do Bitdefender não é a barra habitual do seu navegador. A única coisa que adiciona ao seu navegador é um pequeno arrastador no topo de cada página Web. Clique para ver a barra de ferramentas.

A barra de ferramentas Bitdefender contém os seguintes elementos:

Avaliação da Página

Dependendo de como Bitdefender classifica a página web que está atualmente a ver, uma das seguintes classificações é exibida do lado esquerdo da barra de ferramentas:

- A mensagem "Página Insegura" aparece com um fundo vermelho - deve abandonar a página web imediatamente. Para saber mais acerca desta ameaça, clique no símbolo **+** na página de classificação.
- A mensagem "Recomenda-se cuidado" aparece num fundo laranja - esta página web pode conter conteúdo perigoso. Tenha cuidado se decidir visitá-la.
- A mensagem "Esta página é segura" surge com um fundo verde - esta é uma página segura para visitar.

Sandbox

Clique em para lançar o navegador num ambiente proporcionado pelo Bitdefender, isolando-o do sistema operativo. Isto impede que as ameaças com base no navegador explorem as vulnerabilidades do navegador para obterem o controlo do seu sistema. Use a Sandbox ao visitar as páginas Web que suspeita que contêm malware.

Browser windows aberto em Sandbox será facilmente reconhecido através do seu outline modificado e o ícone Sandbox adicionado ao centro da barra de título.

Nota
A Sandbox não se encontra disponível em computadores com Windows XP.

Definições

Clique em para selecionar características individuais a ativar ou desativar:

- Filtro Antiphishing
- Filtro Web Antimalware
- Consultor de Procura

Botão de Alimentação

Para ativar/desativar totalmente as características da barra de ferramentas, clique em no lado direito da barra.

19.2. Alertas de Bitdefender no navegador

Sempre que tenta visitar uma página Web classificada como insegura, esta é bloqueada e é apresentada uma página de aviso no seu navegador.

A página contém informações como a URL do site web e a ameaça detetada.

Tem de decidir o que fazer a seguir. Estão disponíveis as seguintes opções:

- Navegue para fora da página web clicando em **Leve-me de volta à segurança**.
- Desativar o bloquear de páginas que contenham phishing ao clicar em **Desativar filtro Antiphishing**.
- Desativar o bloquear de páginas que contenham malware ao clicar em **Desativar filtro Antimalware**.
- Adicione a página à lista branca Antiphishing, clicando em **Adicionar à Lista Branca**. Esta página já não será analisada pelos motores Antiphishing do Bitdefender.
- Prosseguir para a página web, apesar do aviso, clicando em **Eu compreendo os riscos, avançar de qualquer forma**.

20. PROTEÇÃO DE DADOS

A proteção de dados evita as fugas de dados sensíveis quando se encontra online.

Imagine a seguinte situação: criou uma regra de proteção de dados para proteger o número do seu cartão de crédito. Se o software spyware consegue instalar no seu computador, não consegue enviar o número de cartão de crédito por email, mensagens instantâneas ou páginas web. Além disso, os seus filhos não o podem usar para adquirir online ou revelar isso às pesoas que encontramos na Internet.

20.1. Acerca da proteção de dados

Quer seja o seu e-mail o seu número de cartão de crédito, quando eles caem em mãos erradas essa informação poderá causar-lhe danos: poderá encontrar-se afogado em mensagens spam ou poderá ser surpreendido ao aceder à sua conta e verificar que está vazia.

Com base nas regras que cria, a Proteção de Dados procura no tráfego da web, email e mensagens instantâneas que saem do seu computador cadeias de caracteres específicos (por exemplo, o seu número de cartão de crédito). Se houver uma correspondência, a respectiva página web, e-mail ou mensagem instantânea é bloqueada.

Pode criar regras para proteger cada peça de informação que possa considerar pessoal ou confidencial, desde o seu número de telefone ou endereço de e-mail até à sua informação bancária. O Suporte multi-utilizador é fornecido de forma a que os utilizadores de diferentes contas do Windows possam configurar e usar as suas próprias regras. Se a sua conta de Windows é uma conta de administrador, as regras que cria podem ser configuradas para também se aplicarem a utilizadores de outras contas do computador.

20.2. Configurar proteção de dados

Se deseja usar a proteção de dados, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Privacidade**.
3. Clique no módulo de **Proteção de Dados**.

4. Certifique-se de que a proteção de dados está ativada.
5. Criar regras para proteger a sua informação sensível. Para mais informação, por favor consulte o "*Criar regras de proteção de dados*" (p. 127).

20.2.1. Criar regras de proteção de dados

Para criar uma regra, clique no botão **Adicionar regra** e siga o assistente de configuração. Pode navegar pelo assistente utilizando os botões **Seguinte** e **Retroceder**. Para sair do assistente, clique em **Cancelar**.

1. **Descrever Regra**

   Deve definir os seguintes parâmetros:

   - **Nome Regra** - insira o nome da regra no campo editável.
   - **Tipo de Regra** - escolha o tipo de regra (endereço, nome, cartão de crédito, PIN, NSS, etc).
   - **Dados Regra** - insira os dados que quer proteger com a regra no campo editável. Por exemplo, se deseja proteger o seu número de cartão de crédito, insira o mesmo ou parte dele aqui.

     Importante

     Recomendamos que insira pelo menos três caracteres de forma a evitar o bloqueio por engano de mensagens e páginas web. Entretanto, para maior segurança, insira apenas dados parciais (por exemplo, apenas parte do número do seu cartão de crédito).

   - **Descrição da regra** - insira uma breve descrição da regra no campo de edição. Um vez que os dados bloqueados (string de caracteres) não são mostrados em pleno texto quando se acede à regra, a descrição deverá ajudá-lo a identificá-la facilmente.

2. **Configurar definições de regra**

   a. Selecione o tráfego que quer que o Bitdefender analise.

   - **Analisar Web (tráfego HTTP)** - analisa o tráfego HTTP (web) e bloqueia os dados de saída que correspondem aos dados da regra.
   - **Analisar e-mail (tráfego SMTP)** - analisa todo o tráfego SMTP (mail) e bloqueia as mensagens de e-mail de saída que contém os dados da regra.

Pode escolher aplicar a regra apenas se a mesma corresponder em todas as palavras ou se os dados da regra e os caracteres detetados correspondem em termos de letra (Maiúsculas, minúsculas).

b. Especifique para que utilizadores se aplicam as regras.

- **Apenas para mim (utilizador atual)** - a regra será aplicada à sua conta de utilizador.
- **Todos os utilizadores** - a regra será aplicada a todas contas do Windows.
- **Utilizadores limitados** - a regra será aplicada a si e a todas as contas de Windows limitadas.

Clique em **Terminar**. A regra aparecerá na tabela.

De agora em diante, qualquer tentativa de enviar os dados da regra pelos protocolos selecionados, irá falhar. Será apresentada uma entrada na janela Eventos indicando que o Bitdefender bloqueou conteúdo específico de uma identidade de ser enviado.

20.3. Gerir regras

Para gerir as regras de proteção de dados:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Privacidade**.
3. Clique no módulo de **Proteção de Dados**.

Pode ver as regras criadas até agora listadas na tabela.

Para apagar uma regra, selecione-a e clique no botão **Remover regra**.

Para editar uma regra, selecione-a e clique no botão **Editar regra**. Uma nova janela irá aparecer. Aqui pode mudar o nome, descripção e parâmetros da regra (tipo, dados e tráfego). Clique em **Aplicar** para guardar as alterações.

20.4. Apagar ficheiros permanentemente

Quando apaga um ficheiro, o mesmo já não fica acessível por meios normais. No entanto o ficheiro continua armazenado no disco duro até que seja sobrescrito quando copiar para lá novos ficheiros.

O Destruidor de Ficheiros do Bitdefender vai ajudar a eliminar permanentemente dados removendo-os fisicamente do seu disco rígido.

Pode rapidamente destruir ficheiros ou pastas do seu computador usando o menu contextual Windows, seguindo os seguintes passos:

1. Clique botão direito sobre o ficheiro ou pasta que deseja apagar permanentemente.
2. Selecione **Bitdefender** > **Destruidor Ficheiros** no menu contextual que aparece.
3. A janela de confirmação irá aparecer. Clique em **Sim** para iniciar o assistente do Destruidor de Ficheiros.
4. Aguarde que o Bitdefender termine a destruição dos ficheiros.
5. Os resultados são apresentados. Clique em **Fechar** para sair do assistente.

Alternativamente pode destruir os ficheiros a partir da interface do Bitdefender.

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Privacidade**.
3. No módulo **Proteção de Dados**, selecione **Triturador de Ficheiros**.
4. Siga o assistente do Destruidor de Ficheiros:
   a. **Selecionar ficheiro/pasta**

      Adicione os ficheiros ou as pastas que pretende remover permanentemente.

   b. **Destruir Ficheiros**

      Aguarde que o Bitdefender termine a destruição dos ficheiros.

   c. **Resultados**

      Os resultados são apresentados. Clique em **Fechar** para sair do assistente.

21. VULNERABILIDADE

Um passo importante na proteção do seu computador contra as pessoas e aplicações maliciosas é manter atualizado o seu sistema operativo e as aplicações que usa regularmente. Também deve considerar desativar as definições do Windows que tornam o sistema mais vulnerável ao malware. Mais ainda, para evitar acesso físico não-autorizado ao seu computador, palavras-passe fortes (palavras-passe que não são fáceis de adivinhar) devem de ser criadas para cada conta de utilizador do Windows.

O Bitdefender verifica automaticamente o seu sistema por vulnerabilidades e alerta-o sobre eles. As vulnerabilidades do sistema incluem:

- aplicações desatualizada no seu computador.
- actualizações do Windows em falta.
- Senhas fracas para as contas de utilizador do Windows.

O Bitdefender proporcionar duas formas fáceis de resolver as vulnerabilidades do seu sistema:

- Pode analisar o seu sistema por vulnerabilidades e repará-las passo a passo com a opção **Análise de Vulnerabilidades**.
- Se usar a monitorização da vulnerabilidade automática, pode verificar e resolver vulnerabilidades detetadas na janela Eventos.

Deve verificar e resolver as vulnerabilidades do sistema semanal ou quinzenalmente.

21.1. Procurar vulnerabilidades no seu sistema

Para corrigir as vulnerabilidades do sistema utilizando a opção Análise de Vulnerabilidade, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. No módulo **Vulnerabilidade**, selecione **Análise de Vulnerabilidade**.
4. Aguarde para o Bitdefender analisar as vulnerabilidades do seu sistema. Para interromper o processo de análise, clique no botão **Saltar** na parte superior da janela.
   a. **Atualização de aplicações**

Se a aplicação não estiver atualizada, clique no link fornecido para descarregar a versão mais recente.

Clique em **Ver detalhes** para ver informações sobre a aplicação que necessita de ser atualizada.

b. **Atualizações do Windows**

Clique em **Ver detalhes** para ver uma lista de atualizações críticas do Windows que não estão instaladas no seu computador.

Para iniciar a instalação das atualizações selecionadas, clique em **Instalar atualizações**. Note que a instalação das atualizações poderá demorar um pouco e poderá ser necessário reiniciar o sistema para concluir a instalação. Se necessário, reinicie o sistema quando lhe convier.

c. **Palavras-passe fracas**

Pode ver a lista dos utilizadores de contas Windows configurados no seu computador e o nível de proteção que as suas palavras-passe garantem.

Clique em **Ver detalhes** para modificar as palavras-passe fracas. Pode escolher entre pedir ao utilizador para alterar a palavra-passe da próxima vez que aceder ou ser você a alterar a palavra-passe imediatamente. Para obter uma palavra-passe forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).

No canto superior direito da janela, pode filtrar os resultados de acordo com as suas preferências.

21.2. Usar monitorização de vulnerabilidade automática

O Bitdefender analisa regularmente as vulnerabilidades do seu sistema, em segundo plano, e mantém registos das incidências detetadas na janela Eventos.

Para verificar e resolver os problemas detetados, siga estes passos:

1. Abra a janela de Bitdefender.
2. Clique no ícone na parte superior da janela e selecione **Definições Gerais** do menu suspenso.

3. Na janela **Eventos**, selecione **Vulnerabilidade**.
4. Pode ver a informação detalhada sobre as vulnerabilidades do sistema detetadas. Dependendo da incidencia, para reparar uma vulnerabilidade específica proceda da seguinte forma:
   - Se houver alguma atualização do Windows disponível, clique em **Atualizar agora**.
   - Se uma aplicação estiver desatualizada, clique em **Atualizar agora** para obter a hiperligação para a página de Internet do fornecedor a partir da qual pode instalar a versão mais recente dessa aplicação.
   - Se uma conta de utilizador do Windows tiver uma palavra-passe fraca, clique em **Alterar palavra-passe** para obrigar o utilizador a mudar a palavra-passe no próximo início de sessão ou alterá-la por si mesmo. Para obter uma palavra-passe forte, use uma combinação de maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).
   - Se o recurso Windows Autorun estiver ativado, clique em **Desativar** para o desativar.

Para configurar as definições de monitorização de vulnerabilidade, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Vulnerabilidade**.
4. Clique no botão para ativar ou desativar a análise de Vulnerabilidade.

> **Importante**
> Para ser notificado automaticamente sobre vulnerabilidades do sistema ou de aplicações, mantenha a opção **Análise de Vulnerabilidade** ativada.

5. Escolha as vulnerabilidades do sistema que deseja que sejam regularmente verificadas usando os botões correspondentes.

   Atualizações Críticas do Windows
   Verifique se o seu sistema operativo Windows possui as mais recentes e importantes atualizações de segurança da Microsoft.

Atualização de aplicações

Verifique se as aplicações instaladas no seu sistema estão atualizadas. As aplicações desatualizadas podem ser exploradas por software malicioso, tornando o PC vulnerável a ataques externos.

Palavras-passe fracas

Verifique se as palavras-passe das contas Windows configuradas no sistema são fáceis de descobrir ou não. A definição de palavras-passe difíceis de descobrir (palavras-passe fortes) torna muito difícil a invasão do seu sistema pelos hackers. Uma palavra-passe forte inclui maiúsculas e minúsculas, números e caracteres especiais (tais como #, $ ou @).

Autorun dispositivos media

Verifique o estado do recurso Windows Autorun. Esta característica permite que as aplicações se iniciem automaticamente a partir dos CDs, DVDs, drives USB ou outros dispositivos externos.

Alguns tipos de malware usam Autorun para se propagar automaticamente dos média removíveis do PC. Por isso, recomenda-se a desactivação desta janela.

Nota

Se desativar a monitorização de uma vulnerabilidade específica, as incidências relacionadas deixarão de ser registadas na janela de Eventos.

22. FIREWALL

A Firewall protege o seu computador de tentativas de ligação de saída e entrada não-autorizadas, quer em redes locais quer na Internet. É bastante semelhante a um guarda no seu seu portão - regista as tentativas de ligação e decide quais deve permitir e quais bloquear.

A firewall do Bitdefender usa um conjunto de regras para filtrar dados transmitidos para ou a partir do seu sistema. As regras encontram-se agrupadas em 2 categorias:

Regras gerais
: Regras que determinam os protocolos através dos quais a comunicação é permitida.

  É usado um conjunto de regras por defeito que proporciona uma proteção ótima. Pode editar as regras permitindo ou impedindo as ligações através de determinados protocolos.

Regras da Aplicação
: As regras que determinam como cada aplicação pode aceder aos recursos da rede e à Internet.

  Em condições normais, o Bitdefender cria automaticamente uma regra sempre que uma aplicação tenta aceder à Internet. Também pode adicionar ou editar manualmente regras das aplicações.

Se o seu computador estiver a executar o Windows Vista, Windows 7 ou Windows 8, o Bitdefender atribui automaticamente um tipo de rede a cada ligação de rede que deteta. Dependendo do tipo de rede, a proteção firewall é definida para o nível apropriado para cada ligação.

Para saber mais sobre as definições da firewall para cada tipo de rede e como pode editar as definições de rede, por favor consulte "*Gerir definições da ligação*" (p. 139).

22.1. Ativar/desativar firewall de proteção

Para ativar ou desativar a privacidade da firewall, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Firewall**.

4. Na janela da **Firewall**, clique no botão da Firewall.

Atenção

Porque expõe o seu computador a ligações não autorizadas, desligar a firewall deveria ser uma medida temporária. Volte a ligar a firewall assim que possível.

22.2. Gerir regras da Firewall

22.2.1. Regras gerais

Sempre que determinados dados são transmitidos pela Internet, são usados certos protocolos.

As regras gerais permitem-lhe configurar os protocolos através dos quais o tráfego é permitido. Por defeito, as regras gerais não são apresentadas ao abrir o Firewall. Para editar regras, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Firewall**.
4. Na janela da **Firewall**, selecione o separador **Regras**.
5. Marque a caixa **Exibir regras gerais** no canto inferior esquerdo da janela.

As regras predefinidas são apresentadas. Para editar a prioridade de uma regra, clique na seta correspondente na coluna **Permissão** e selecione **Permitir** ou **Negar**.

DNS sobre UDP / TCP
Permitir ou impedir DNS em vez de UDP e TCP.

Por defeito, este tipo de ligação é permitido.

Entrada de ICMP / ICMPv6
Permitir ou impedir mensagens ICMP / ICMPv6.

As mensagens ICMP são frequentemente usadas pelos hackers para atacarem as redes de computadores. Por defeito, este tipo de ligação é negado.

Enviar emails
Permitir ou impedir envio de email por SMTP.

Por defeito, este tipo de ligação é permitido.

Navegação na Web HTTP
Permitir ou impedir navegação na web HTTP.

Por defeito, este tipo de ligação é permitido.

Entrada de Acesso Remoto ao Computador
Permitir ou impedir o acesso de outros computadores em Ligações Remotas de Desktop.

Por defeito, este tipo de ligação é permitido.

Tráfego do Windows Explorer em HTTP / FTP
Permitir ou impedir tráfego HTTP ou FTP do Windows Explorer.

Por defeito, este tipo de ligação é negado.

22.2.2. Regras da aplicação

Para visualizar e gerir as regras da firewall de controlo do acesso a aplicações a recursos da rede e à Internet, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Firewall**.
4. Na janela da **Firewall**, selecione o separador **Regras**.

Pode ver na tabela os programas (processos) para os quais as regras de firewall foram criadas. Para ver as regras criadas para uma aplicação específica, clique duas vezes nela.

Para cada regra é apresentada a seguinte informação:

- **Nome** - o nome do processo onde as regras se aplicam.
- **Tipos de Rede** - os tipos de processo e de adaptador de rede onde as regras se aplicam. As regras são automaticamente criadas para filtrar o acesso à rede ou à Internet através de qualquer adaptador. Por defeito, as regras aplicam-se a qualquer rede. Pode criar manualmente as regras ou editar as regras existentes para filtrar o acesso à rede ou à Internet de uma aplicação através de um determinado adaptador (por exemplo, um adaptador de rede wireless).
- **Protocolo** - o protocolo IP aos quais as regras se aplicam. Por defeito, as regras aplicam-se a qualquer protocolo.

- **Permissão** - se o acesso à aplicação na rede ou na Internet é permitida ou negada sob circunstâncias específicas.

Para gerir as regras, utilize os botões acima da tabela:

- **Adicionar regra** - abre uma janela onde pode criar uma regra nova.
- **Remover regra** - apaga a regra selecionada.
- **Repor regras** - abre uma janela onde pode optar por remover as regras atuais e restaurar as predefinidas.

Adicionar/ editar regras da aplicação

Para adicionar ou editar uma regra de aplicação, clique no botão **Adicionar regra** acima da tabela ou clique numa regra atual. Uma nova janela irá aparecer. Proceder da seguinte forma:

- **Caminho do Programa.** Clique em **Explorar** para selecionar a aplicação à qual a regra se aplica.
- **Endereço Local.** Especifique o endereço IP local e a porta aos quais a regra se aplica. Se tem mais de um adaptador de rede, pode limpar a caixa de seleção **Todos** e inserir um endereço IP específico.
- **Endereço Remoto.** Especifique o endereço IP remoto e a porta aos quais a regra se aplica. Para filtrar o tráfego entre o seu computador e um determinado computador, limpe a caixa de seleção **Todos** e insira o endereço IP do outro computador.
- **versão IP.** Selecione do menu a versão do IP (IPv4, IPv6 ou qualquer) ao qual a regra se aplica.
- **Direção.** Selecione do menu a direção do tráfego ao qual a regra se aplica.

Direção	Descrição
Saída	A regra aplica-se apenas ao tráfego de saída.
Entrada	A regra aplica-se apenas ao tráfego de entrada.
Ambos	A regra aplica-se em ambos os sentidos.

Clique na hiperligação **Mais opções** para outras ações:

- **Protocolo.** Selecione do menu o protocolo IP ao qual a regra se aplica.
  - Se deseja que a regra se aplique a todos os protocolos, selecione **Todos**.

- Se deseja que a regra se aplique ao TCP, selecione **TCP**.
- Se deseja que a regra se aplique ao UDP, selecione **UDP**.
- Se quiser que a regra se aplique num protocolo específico, introduza o número atribuído ao protocolo que quiser filtrar no campo de edição em branco.

> **Nota**
>
> Os números dos protocolos IP são atribuídos pelo Internet Assigned Numbers Authority (IANA). Pode encontrar a lista completa de números IP atribuidos em http://www.iana.org/assignments/protocol-numbers.

- **Eventos.** Dependendo dos protocolo selecionado, escolha os eventos de rede aos quais a regra se aplica. Os seguintes eventos podem ser tidos em consideração:

Evento	Descrição
Ligar	Intercâmbio preliminar de mensagens standard usado pelos protocolos orientados para a ligação (tais como TCP) para estabelecer a mesma. Com protocolos orientados para a ligação, o tráfego de dados entre dois computadores ocorre apenas após a ligação ser estabelecida.
Tráfego	Fluxo de dados entre dois computadores.
Escutar	Estado em que uma aplicação monitoriza a rede à espera de estabelecer uma ligação ou de receber informação de uma aplicação parceira.

- **Tipo de rede.** Selecione o tipo de rede ao qual a regra se aplica. Pode alterar o tipo abrindo o menu pendente **Tipo de Rede** e selecionando um dos tipos disponíveis na lista.

Tipo de rede	Descrição
Fidedigna	Desativa a firewall para o respetivo dispositivo.
Casa/Escritório	Permite o tráfego entre o seu computador e os computadores na rede local.
Público	Todo o tráfego é filtrado.

Tipo de rede	Descrição
Não fidedigna	Bloqueia completamente o tráfego de rede e de Internet através do respetivo adaptador.

- **Permissão.** Selecione uma das seguintes permissões disponíveis:

Permissão	Descrição
Permitir	À aplicação especificada será permitido o acesso à rede / Internet nas circunstâncias determinadas.
Bloquear	À aplicação especificada será negado o acesso à rede / Internet nas circunstâncias determinadas.

22.3. Gerir definições da ligação

Para cada ligação de rede pode configurar as zonas fidedignas e não fidedignas.

Uma zona fidedigna é um dispositivo em que confia plenamente, por exemplo um computador ou uma impressora. Todo o tráfego entre o seu computador e o dispositivo fidedigno é permitido. Para partilhar recursos com determinados computadores numa rede wireless insegura, adicione-os como computadores autorizados.

Uma zona não fidedigna é um dispositivo que você não quer de forma alguma com o seu.

Para visualizar e gerir zonas na sua rede de adaptadores, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Firewall**.
4. Na janela da **Firewall**, selecione o separador **Adaptadores**.

Aparecerá uma nova janela que lhe mostra os adaptadores de rede com ligações ativas e as atuais zonas, se houver algum.

Para cada zona a seguinte informação é exibida:

- **Tipo de Rede** - o tipo de rede a que o seu computador está ligado.

- **Modo Stealth** - para não ser detetado por outros computadores.

  Para configurar o Modo Stealth, selecione a opção desejada do menu correspondente.

Opção Stealth	Descrição
Em	O Modo Escondido está ligado. O seu computador é invisível a partir da rede local e da Internet.
Desligado	O Modo Escondido está desligado. Qualquer pessoa da rede local ou da Internet pode fazer ping e detetar o seu computador.
Remoto	O seu computador não pode ser detetado da Internet. As redes locais podem fazer ping e detetar o seu computador.

- **Genérico** - se as regras genéricas são aplicadas a esta ligação.

  Se o endereço IP de um adaptador é alterado, o Bitdefender modifica o tipo de rede de acordo com a alteração. Se deseja manter o mesmo tipo, selecione **Sim** do menu correspondente.

Adicionar/editar exceções

Para adicionar ou editar exceções, clique no botão **Exceções de rede** acima da tabela. Surgirá uma nova janela apresentando os endereços IP dos dispositivos ligados à rede. Proceder da seguinte forma:

1. Selecione o endereço IP do computador que deseja adicionar ou digite o endereço ou address range na caixa de texto providenciada.
2. Selecione a permissão:
   - **Permitir** - para autorizar o tráfego entre o seu computador e o computador selecionado.
   - **Negar** - para bloquear o tráfego entre o seu computador e o computador selecionado.
3. Clique no botão + para adicionar a exceção, guardar e fechar a janela.

   Se quiser retirar um IP, clique no botão correspondente e feche a janela.

22.4. Configurar definições avançadas

Para configurar as definições avançadas de firewall, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Firewall**.
4. Na janela da **Firewall**, selecione o separador **Definições**.

As seguintes funcionalidades podem ser ativadas ou desativadas.

- **Internet Connection Sharing** - ativa o suporte para o Internet Connection Sharing.

  > **Nota**
  > Esta opção não ativa automaticamente o **Internet Connection Sharing** no seu sistema, mas apenas permite este tipo de ligação em caso de a ativar no seu sistema operativo.

- **Bloquear scans das portas na rede** - deteta e bloqueia tentativas de encontrar quais portas encontram-se abertas.

  Os scans de portas são frequentemente usados pelos hackers para descobrir que portas se encontram abertas no seu computador. Então eles poderão entrar no seu computador se descobrirem uma porta menos segura ou vulnerável.

- **Monitorizar notificações wireless** - quando está ligado a redes wireless, a informação é apresentada sobre eventos específicos de rede (por exemplo, quando um novo computador foi ligado à rede).

22.5. Configurar intensidade de alertas

Bitdefender Internet Security 2015 foi concebido para ser o mínimo intrusivo possível. Em condições normais, não necessita de tomar decisões sobre permitir ou impedir ligações ou ações tentadas pelas aplicações em execução do seu sistema.

Se quiser ter o controlo total sobre a decisão, siga os seguintes passos:

1. Abra a janela de Bitdefender.

2. Clique no ícone na parte superior da janela e selecione **Definições Gerais** do menu suspenso.
3. Na janela **Definições Gerais** selecione o separador **Definições Gerais**.
4. Ligar **Modo Paranóico** clicando no botão correspondente.

> **Nota**
> Quando o modo Paranóico está ligado, os recursos Autopilot e Perfis serão automaticamente desligados.
> O **Modo Paranoico** poderá ser usado simultaneamente com o **Modo de Bateria**.

Enquanto o Modo Paranóico estiver ligado,você receberá notificações para tomar uma ação sempre que uma das seguintes situações ocorre:

- Uma aplicação tenta ligar à Internet.
- Uma aplicação tenta realizar uma ação considerada suspeita pelo Deteção de intrusão ou pelo Controlo ativo de vírus.

O alerta contém informações detalhadas sobre a aplicação e o comportamento detetado. Selecione para **Permitir** ou **Impedir** a ação usando o botão respetivo.

23. DETEÇÃO DE INTRUSÃO

A Detecção de Invasão do Bitdefender monitoriza as atividades da rede e do sistema por atividades maliciosas ou violações da política. Pode detetar e bloquear as tentativas de alterar ficheiros críticos do sistema, ficheiros do Bitdefender ou entradas de registo, a instalação de drivers de malware ou ataques efetuados por injeção de código (injeção da DLL).

Para configurar a Detecção de Invasão, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Detecção de Invasão**.
4. Para ativar a Detecção de Invasão, clique no botão correspondente.
5. Arraste o cursor pela escala para definir o nível de agressividade pretendido. Utilize a descrição do lado direito da escala para escolher o nível que melhor se adequa às suas necessidades de segurança.

Pode verificar que aplicações foram detetadas pela Detecção de Invasão na janela Eventos.

Se existirem aplicações em que confie e que não quer que a Detecção de Invasão analise, pode adicionar regras de exclusão para elas. Para excluir uma aplicação da análise, siga os passos descritos na secção *"Gerir processos excluídos"* (p. 110).

Nota

A operação da Detecção de Invasão está relacionada com a do Controlo Ativo de Vírus. As regras de exclusão de processo aplicam-se a ambos os sistemas.

24. SEGURANÇA SAFEPAY PARA TRANSAÇÕES ONLINE

O computador está a tornar-se na principal ferramenta para a realização de compras e operações bancárias. Pagar contas, transferir dinheiro, comprar praticamente qualquer coisa que possa imaginar nunca foi tão fácil e rápido.

Isto engloba enviar informação pessoal, de conta e de cartão de crédito, palavras-passe e outros tipos de informação privada pela Internet, por outras palavras exatamente o tipo de fluxo de informação que os cibercriminosos estão muito interessados em deitar a mão. Os hackers são incansáveis nos seus esforços para roubar esta informação, assim que nunca poderá ser demasiado cuidadoso em manter seguras as suas transações online.

O Bitdefender Safepay™ é, acima de tudo, um navegador protegido, um ambiente desenhado para manter a sua atividade bancária, as suas compras online e qualquer outra transação online privada e segura.

Para a melhor proteção da privacidade, a Carteira do Bitdefender foi integrada ao Bitdefender Safepay™ para proteger as suas credenciais quando quiser aceder a locais online privados. Para mais informação, por favor consulte o "*Proteção de Carteira para as suas credenciais*" (p. 149).

O Bitdefender Safepay™ oferece as seguintes funcionalidades:

- Bloqueia o acesso ao seu ambiente de trabalho e de qualquer tentativa de tirar fotografias do seu ecran.
- Protege as suas palavras-passe secretas enquanto navega online com a Carteira.
- Vem com um teclado virtual que, quando usado, torna impossível para os hackers lerem as teclas que usar.
- É completamente independente dos outros navegadores.
- Vem com uma proteção hotspot inbuída para ser usada quando o seu computador se liga a redes Wi-fi não-seguras.
- Suporta bookmarks e permite-lhe navegar entre os seus sites favoritos de bancos/compras.
- Não está só limitado ao banking e às compras online. Qualquer página Web pode ser aberta no Bitdefender Safepay™.

24.1. A utilizar o Bitdefender Safepay™

Por defeito, o Bitdefender deteta quando entra numa página de um banco ou de compras em qualquer navegador do seu computador e pergunta se gostaria de utilizar o Bitdefender Safepay™.

Para aceder à interface principal do Bitdefender Safepay™, utilize um dos métodos a seguir:

- A partir da interface do Bitdefender:
  1. Abra a janela de Bitdefender.
  2. Clique no botão **Safepay** à direita na janela.
- Do Windows:
  - No **Windows XP**, **Windows Vista** e **Windows 7**:
    1. Clique em **Iniciar** e vá para **Todos os Programas**.
    2. Clique em **Bitdefender**.
    3. Clique em **Bitdefender Safepay™** ou, mais rápido, clique no botão de ação do **Safepay** à direita na interface do Bitdefender.
  - No **Windows 8**:

    Encontre o Bitdefender Safepay™ no Ecrã inicial do Windows (por exemplo, pode introduzir "Bitdefender Safepay™" diretamente no Ecrã Inicial) e, em seguida, clique no ícone. Alternativamente, pode clicar no botão de ação do **Safepay** à direita na interface do Bitdefender.

> **Nota**
> Se o plug-in do Adobe Flash Player não estiver instalado ou estiver desatualizado, será apresentada um mensagem do Bitdefender. Clique no botão correspondente para continuar.
> Após o processo de instalação, terá que reabrir o navegador Bitdefender Safepay™ manualmente para continuar com o seu trabalho.

Se estiver habituado a navegadores da Internet, não terá nenhum problema em utilizar o Bitdefender Safepay™ - ele parece e comporta-se como um navegador normal:

- insira URLs que deseja ir na barra de endereços.
- adicione separadores para visitar múltiplas páginas na janela do Bitdefender Safepay™ clicando em .

- navegue para a frente e para trás e atualize as páginas usando respetivamente.
- aceda a Definições do Bitdefender Safepay™ clicando em .
- proteja as suas palavras-passe com Carteira clicando em .
- pode gerir os seus bookmarks clicando em ao lado da barra de endereço.
- pode abrir o teclado virtual clicando em .
- aumente ou diminua o tamanho do navegador pressionando as teclas **Ctrl** e **+/-** simultaneamente no teclado numérico.

24.2. Configurar definições

Clique em para configurar as seguintes definições:

Comportamento geral do Bitdefender Safepay™

Escolha o que deve de ser feito quando acede a um site online de compras ou de bancos no seu navegador habitual:

- Abrir automaticamente no Bitdefender Safepay™.
- Que o Bitdefender o avise para a ação a tomar.
- Nunca utilize o Bitdefender Safepay™ para páginas visitadas num navegador normal.

Lista de domínios

Escolha como o Bitdefender Safepay™ irá comportar-se quando visitar páginas com domínios específicos no seu navegador adicionando-os à lista de domínios e selecionando o comportamento para cada um deles:

- Abrir automaticamente no Bitdefender Safepay™.
- Que o Bitdefender o avise para a ação a tomar.
- Nunca utilizar o Bitdefender Safepay™ ao visitar uma página do domínio num navegador normal.

A bloquear pop-ups

Pode escolher para bloquear pop-ups clicando no botão correspondente.

Também pode criar uma lista de páginas que possa permitir pop-ups. A lista deve conter apenas os sites web em que confia plenamente.

Para adicionar uma página à lista, introduza o seu endereço no campo correspondente e clique em **Adicionar domínio**.

Para remover um site web desta lista, selecione-o na lista e clique na hiperligação **Remover** correspondente.

24.3. Gerir bookmarks

Se desativou a detecção automática de alguma ou de todas as páginas, ou o Bitdefendersimplesmente não detectar algumas páginas, pode adicionar bookmarks ao Bitdefender Safepay™ para que possa abrir facilmente as suas páginas favoritas no futuro.

Siga estes passos para adicionar um URL aos bookmarks do Bitdefender Safepay™

1. Clique ao lado da barra de endereço para abrir a página dos Bookmarks.

   Nota
   A página de Bookmarks abre por defeito quando executa o Bitdefender Safepay™.

2. Clique no botão **+** para adicionar um novo bookmark.
3. Inserir o URL e o título do bookmark e clique em **Criar**. O URL é também adicionado à lista de Domínios na página de definições.

24.4. Proteção Hotspot em redes não-seguras.

Quando utilizar o Bitdefender Safepay™ em redes Wi-fi inseguras (por exemplo, um hotspot público), é oferecida uma proteção extra através da característica Proteção de Hotspot. Este serviço encripta as comunicações Internet em ligações não-seguras, ajudando assim a manter a sua privacidade sem importar a que rede esteja ligado.

Os seguintes pré-requisitos tem de ser satisfeitos para que a proteção Hotspot funcione:

- Entrou na sua conta MyBitdefender a partir do Bitdefender Internet Security 2015.
- O seu computador está ligado a uma rede não-segura.

Uma vez que se verifiquem os pré-requisitos, o Bitdefender irá perguntar se deseja utilizar uma ligação segura ao abrir o Bitdefender Safepay™. Tudo o que necessita de fazer é inserir as suas credenciais da MyBitdefender quando solicitado.

A ligação segura será iniciada e uma mensagem irá aparecer na janela do Bitdefender Safepay™ quando a ligação for estabelecida. O símbolo aparece à frente do URL na barra de endereços para o ajudar a identificar facilmente as ligações seguras.

Para melhorar a sua experiência de navegação, pode escolher ativar os plug-ins do **Adobe Flash** e do **Java** clicando em **Mostrar definições avançadas**.

Pode ser necessário confirmar a ação.

25. PROTEÇÃO DE CARTEIRA PARA AS SUAS CREDENCIAIS

Utilizamos os nossos computadores para efetuar compras online ou pagar as contas, para nos ligarmos a plataformas de comunicação social ou para iniciar sessão em aplicações de mensagens instantâneas.

Mas como todos sabemos, nem sempre é fácil memorizar a palavra-passe!

E se não formos cuidadosos ao navegar online, as nossas informações privadas, tais como endereço de e-mail, ID de mensagens instantâneas ou os dados do cartão de crédito, podem ficar comprometidas.

Guardar as suas palavras-passe ou os seus dados pessoais numa folha ou no computador pode ser perigoso, pois podem ser acedidos e utilizados por pessoas que pretendam roubar e utilizar essas informações. E memorizar todas as palavras-passe definidas para as suas contas online ou para os seus sites Web favoritos não é uma tarefa fácil.

Portanto, há alguma forma de garantir que encontramos as nossas palavras-passe quando necessitamos das mesmas? E podemos ter a certeza de que as nossas palavras-passe secretas estão sempre seguras?

Carteira é o gestor de palavras-passe que o ajuda a controlar as suas palavras-passe, protege a sua privacidade e proporciona uma experiência de navegação segura.

Utilizando uma única palavra-passe principal para aceder às suas credenciais, a Carteira simplifica a proteção das suas palavras-passe.

Para oferecer a melhor proteção para as suas atividades online, a Carteira está integrada com o Bitdefender Safepay™ e fornece uma solução única para as várias maneiras com que os seus dados pessoais podem ficar comprometidos.

A Carteira protege as seguintes informações privadas:

- Informações pessoais, tais como endereço de e-mail e número de telefone
- Credenciais de início de sessão dos sites Web
- Informações de contas bancárias ou o número do cartão de crédito
- Dados de acesso às contas de e-mail
- Palavras-passe das aplicações

- Palavras-passe das redes Wi-Fi

25.1. Configurar a Carteira

Após a conclusão da instalação e aquando da abertura do seu navegador, será notificado através de uma janela emergente que pode utilizar a Carteira para uma experiência de navegação mais simples.

Clique em **Explorar** para iniciar o assistente de configuração para a Carteira. Siga o assistente para concluir o processo de configuração.

Podem ser executadas duas tarefas adicionais durante este passo:

- Crie uma nova base de dados de Carteira para proteger as suas palavras-passe.

  Durante o processo de configuração, ser-lhe-á solicitada a proteção da sua Carteira com uma palavra-passe principal. A palavra-passe deve ser segura e conter pelo menos 6 carateres.

  Para criar uma palavra-passe segura utilize no mínimo um número ou símbolo e uma maiúscula. Após definir a palavra-passe, se alguém tentar aceder à Carteira terá de inserir primeiro a palavra-passe.

  No final do processo de configuração, são ativadas por predefinição as seguintes definições da Carteira:

  - **Guardar automaticamente as credenciais na Wallet**.
  - **Solicitar a minha palavra-passe principal quando iniciar sessão no meu computador**.
  - **Bloquear automaticamente a Wallet quando deixar o meu PC sem supervisão**.
- Importe uma base de dados existente caso já tenha utilizado anterior a Carteira no seu sistema.

Exportar a base de dados da Carteira

Para exportar a base de dados da Carteira, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Privacidade**.
3. No módulo **Carteira**, selecione **Exportar Carteira**.

4. Siga os passos para exportar a base de dados da Carteira para uma localização no seu sistema.

Criar uma nova base de dados Carteira

Para criar uma nova base de dados da Carteira, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Privacidade**.
3. No módulo **Carteira> a**, selecione **Criar Nova Carteira**.
4. Será apresentada uma janela de aviso informando que os dados atuais armazenados na Carteira serão eliminados. Clique em **Sim** para limpar a base de dados existente e para continuar com o assistente. Para sair do assistente, clique em **Não**.

Gerir as suas credenciais da Carteira

Para gerir as suas palavras-passe, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Privacidade**.
3. No módulo **Carteira**, selecione **Abrir Carteira**.

Uma nova janela irá aparecer. Selecione a categoria pretendida na parte superior da janela:

- Identidade
- Websites
- Online banking
- Cliente e-mail
- Aplicações
- Redes Wi-Fi

Adicionar/editar as credenciais

- Para adicionar uma nova palavra-passe, escolha a categoria pretendida acima, clique em **+ Adicionar item**, insira as informações nos campos correspondentes e clique no botão Guardar.

- Para editar uma entrada da lista, selecione-a e clique no botão **Editar**.
- Para sair, clique em **Cancelar**.
- Para remover uma entrada, selecione-a, clique no botão **Editar** e escolha **Eliminar**.

25.2. Ligar ou desligar a proteção da Carteira

Para ligar ou desligar a proteção da Carteira, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Privacidade**.
3. Clique no módulo **Carteira**.
4. Na janela **Carteira**, clique no botão para ativar ou desativar **Carteira**.

25.3. Gerir as definições da Carteira

Para configurar a palavra-passe principal detalhadamente, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Privacidade**.
3. Clique no módulo **Carteira**.
4. Na janela **Carteira**, selecione o separador **Palavra-passe Principal**.

Estão disponíveis as seguintes opções:

- **Solicitar a minha palavra-passe principal sempre que eu aceder ao meu PC** - ser-lhe-á solicitado a introduzir a palavra-passe principal ao aceder ao computador.
- **Solicitar palavra-passe principal quando abro browsers e aplicações** - ser-lhe-á solicitada a introdução da palavra-passe principal quando acede a um browser ou aplicação.
- **Bloquear automaticamente a Carteira quando deixo o meu PC sem supervisão** - ser-lhe-á solicitada a introdução da palavra-passe principal quando regressar ao seu computador após 15 minutos.

Importante
Não se esqueça da sua palavra-passe principal e registe-a num local seguro. Se esquecer a palavra-passe, terá de reinstalar o programa ou contactar o apoio do Bitdefender.

Melhore a sua experiência

Para selecionar os browsers ou as aplicações nos quais pretende integrar a Carteira, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Privacidade**.
3. Clique no módulo **Carteira**.
4. Na janela **Carteira**, selecione o separador **Aplicações melhoradas**.

   Verifique uma aplicação para utilizar a Carteira e melhorar a sua experiência:

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - Safepay
   - Yahoo! Messenger
   - Skype

Configurar o Preenchimento automático

A funcionalidade Preenchimento automático simplifica a ligação aos seus sites Web favoritos ou o início de sessão nas suas contas online. A primeira vez que introduzir as suas credenciais de início de sessão e informações pessoais no navegador da Internet, estes estarão automaticamente protegidos na Carteira.

Para configurar as definições do **Preenchimento automático**, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Privacidade**.
3. Clique no módulo **Carteira**.
4. Na janela **Carteira**, selecione o separador**Definições de preenchimento automático**.
5. Configure as seguintes opções:

   - **Preencher automaticamente as credenciais de início de sessão**:

- **Preencher automaticamente e sempre as credenciais de início de sessão** - ao credenciais são inseridas automaticamente no browser.
- **Deixe-me decidir quando quero preencher automaticamente as minhas credenciais de início de sessão** - pode escolher quando preencher as credenciais automaticamente no navegador.

- **Configure como a Carteira protege as suas credenciais**:
  - **Guardar credenciais automaticamente na Carteira** - as credenciais de início de sessão e outras informações pessoais como os detalhes do seu cartão de crédito e detalhes pessoais são guardados e atualizados automaticamente na sua Carteira.
  - **Perguntar-me sempre** - ser-lhe-á sempre perguntado se pretende adicionar as suas credenciais à Carteira.
  - **Não guardar, atualizarei as informações manualmente** - as credenciais só podem ser atualizadas na Carteira manualmente.
- **Formulários de preenchimento automático**:
  - **Mostrar as minhas opções de preenchimento quando eu visitar uma página com formulários** - um pop-up com as opções de preenchimento irá aparecer sempre que o Bitdefender detetar que deseja realizar um pagamento online ou iniciar a sessão.

Gerir as informações da Carteira, a partir do seu navegador

Pode gerir facilmente a sua Carteira diretamente do seu navegador para ter todos os dados importantes à mão. O add-on da Carteira é suportado pelos seguintes navegadores: Google Chrome, Internet Explorer e Mozilla Firefox, e está também integrado com o Safepay.

Para aceder à extensão da Carteira, abra o seu navegador, permita que o add-on seja instalado e clique no ícone na barra de ferramentas.

A extensão da Carteira contém as seguintes opções:

- Abrir Carteira - abre a Carteira.
- Bloquear Carteira - bloqueia a Carteira.
- Sites Web - abre um submenu com todos os inícios de sessão em sites Web armazenados na Carteira. Clique em **Adicionar sites Web** para adicionar novos sites Web à lista.

- Preencher formulários - abre o submenu que contém as informações que adicionou para uma categoria específica. Aqui pode adicionar novos dados à sua Carteira.
- Definições - abre a janela de definições da Carteira.
- Relatar problema - relata qualquer problema encontrado com a Carteira do Bitdefender.

26. CONTROLO PARENTAL

O Controlo Parental Bitdefender permite-lhe controlar o acesso à Internet e a determinadas aplicações para cada conta de utilizador no sistema.

Assim que configurar o Controlo Parental, poderá facilmente saber o que o seu filho está a fazer no computador.

Tudo o que precisa é um computador com acesso à Internet e um navegador de Internet.

Pode configurar o Controlo Parental para bloquear:

- Páginas web inapropriadas.
- ligação à Internet, durante determinados períodos de tempo (tal como o período de estudo).
- aplicações tais como: jogos, programas de partilha de ficheiros e outros.
- mensagens instântaneas enviadas por contacto IM para além dos que estão permitidos.

Verifique a atividade dos seus filhos e altere as definições do controlo Parental usando a MyBitdefender a partir de qualquer computador ou dispositivo móvel ligado à Internet.

26.1. Aceder ao Painel do Controlo Parental

O painél do Controlo Parental está organizado em módulos a partir dos quais pode monitorizar a atividade dos seus filhos no computador.

O Bitdefender permite-lhe controlar o acesso à Internet e a determinadas aplicações por parte do seu filho. Ao mesmo tempo, permite-lhe monitorizar a atividade da sua conta no Facebook.

Com o Bitdefender pode aceder às definições do Controlo Parental a partir da sua conta MyBitdefender em qualquer computador ou dispositivo móvel ligado à Internet.

Aceder à sua conta online:

- Em qualquer dispositivo com acesso à Internet:
  1. Abrir um browser web.
  2. Vá para:https://my.bitdefender.com

3. Inicie sessão na sua conta com o seu nome de utilizador e palavra-passe.
4. Clique em **Controlo Parental** para aceder ao painel.

- A partir do interface do Bitdefender :

1. Certifique-se que tem a sessão iniciada com a conta de administrador. Apenas os utilizadores com direitos de administrador no sistema podem aceder e configurar o Controlo Parental.
2. Abra a janela de Bitdefender.
3. Aceda ao painel de **Privacidade**.
4. No módulo **Controlo Parental**, selecione **Configurar**.

   Certifique-se de que tem sessão iniciada na sua conta MyBitdefender.
5. O painel do Controlo Parental abrirá numa nova janela. Aqui pode verificar e configurar as definições do Controlo Parental de cada conta de utilizador do Windows.

26.2. Adicionar o perfil do seu filho

Antes de configurar o Controlo Parental, crie contas de utilizador do Windows separadas para os seus filhos. Isto permitir-lhe-á saber o que cada um faz no computador. Deve criar contas de utilizador limitadas (padrão) para que não possam alterar as definições do Controlo Parental. Para mais informação, por favor consulte o "*Como posso criar contas de utilizador do Windows?*" (p. 69).

Para adicionar o perfil do seu filho ao Controlo Parental:

1. Aceda ao painel do Controlo Parental a partir da sua conta MyBitdefender.
2. Clique em **Adicionar Filho** do lado esquerdo do menu.
3. Introduza o nome e idade da criança nos campos correspondentes. A definição da idade da criança vai carregar automaticamente as definições consideradas adequadas para essa faixa etária, com base nos padrões de desenvolvimento infantil.
4. Pode visualizar abaixo os dispositivos ligados à sua conta MyBitdefender.
5. Selecione o computador e a conta Windows para o seu filho.
6. Clique em **Criar Perfil**.

O computador e a conta Windows do seu filho estão agora ligados à sua conta MyBitdefender.

26.2.1. Instalar o Controlo Parental no dispositivo Android

Para instalar o Controlo Parental no dispositivo móvel do seu filho, siga estes passos:

1. Aceda ao painel do Controlo Parental a partir da sua conta MyBitdefender.
2. Clique em **Adicionar Filho** do lado esquerdo do menu.
3. Introduza o nome e idade da criança nos campos correspondentes. A definição da idade da criança vai carregar automaticamente as definições consideradas adequadas para essa faixa etária, com base nos padrões de desenvolvimento infantil.
4. Clique em **Instalar no novo dispositivo** para continuar.
5. Uma nova janela irá aparecer. Selecione **Google Play** na lista.
6. Para transferir e instalar o Controlo Parental no dispositivo, clique no botão **Instalar**.
7. Selecione o dispositivo onde pretende instalar a aplicação.
8. Clique em **Instalar** para continuar.

   Aguarde a instalação da aplicação no dispositivo. Certifique-se de que o dispositivo da criança está ligado à Internet.
9. No final da instalação, ser-lhe-á solicitado o fornecimento dos direitos de administrador da aplicação no dispositivo.
10. Toque em **Aceitar** para concluir a instalação.

Ligar o Controlo Parental a MyBitdefender

Para monitorizar a atividade online do seu filho, deve associar o dispositivo do seu filho à sua conta MyBitdefender ao iniciar sessão na conta à partir da aplicação.

Para associar o dispositivo à sua conta MyBitdefender, siga estes passos:

1. Introduza o nome de utilizador e a palavra-passe da sua MyBitdefender.

   Caso não possua uma conta, opta por criar uma nova conta utilizando o botão correspondente.

Nota
Também pode introduzir um nome para o seu dispositivo. Caso associe mais de um dispositivo à sua conta, isso irá ajudar a identificar os dispositivos com maior facilidade.

2. Toque em **Iniciar sessão**.

   O dispositivo do seu filho está agora ligado à sua conta MyBitdefender e pode começar a monitorizar as suas atividades online.

26.2.2. Monitorizar a atividade da criança

O Bitdefender ajuda a controlar o que os seus filhos fazem online.

Desta forma, pode sempre descobrir exatamente que websites eles visitaram, que aplicações usaram ou que atividades foram bloqueadas pelo Controlo Parental.

Os relatórios contém informação detalhada para cada evento, tal como:

- O estado do evento.
- O nome do website bloqueado.
- O nome da aplicação bloqueada.
- O nome do dispositivo.
- A data e a hora em que ocorreu o evento.
- As ações levadas a cabo pelo Bitdefender.

Para monitorizar o tráfego Internet, as aplicações acedidas ou a atividade do facebook do seu filho, faça o seguinte:

1. Aceda ao painél do Controlo Parental a partir da sua conta MyBitdefender.
2. Clique em para aceder à janela de atividade para o módulo correspondente.

26.2.3. Configurar as Definições Gerais

- Relatórios de atividade

  Por defeito, quando o Controlo Parental está activado, as actividades dos seus filhos são registadas.

  Para receber notificações por e-mail, faça o seguinte:

1. Aceda ao painél do Controlo Parental a partir da sua conta MyBitdefender.
2. Clique no ícone em **Definições Gerais** no canto superior direito.
3. Ative a opção correspondente para receber relatórios de atividade.
4. Introduza o endereço eletrónico para onde serão enviadas das notificações por correio eletrónico.
5. Ajuste a frequência ao selecionar: diariamente, semanalmente ou mensalmente.
6. Receber notificações por e-mail para o seguinte:
   - Sites Web bloqueados
   - App bloqueadas
   - Contactos MI bloqueados
   - SMS de um contacto bloqueado
   - Chamada recebida de um número bloqueado
   - Remoção da aplicação Controlo Parental para Facebook
7. Clique em **Guardar**.

- Informações da Conta

  Observe a área **Informações de conta**. Poderá visualizar o estado de registo, a chave de licença atual e data de expiração.

- Ative a opção para atualizar os agentes instalados nos seus dispositivos e ajustar a frequência ao selecionar: diária, semanal ou mensalmente.

Nota
Selecione a Caixa de verificação correspondente para ocultar o Ecrã de boas-vindas.

26.3. Configurar Controlo Parental

O painél do Controlo Parental é de onde pode gerir diretamente os módulos do Controlo Parental.

cada módulo contém os seguintes elementos: o nome do módulo, uma mensagem de estado, o ícone do módulo e um botão que lhe permite levar a cabo as tarefas mais importantes relacionadas com o módulo.

Clique num separador para configurar as funcioladidades do Controlo Parental correspondentes ao computador:

- Web - para filtrar a navegação na web e definir as restrições de tempo no acesso à Internet.
- Aplicações - para bloquear ou restringir o acesso a aplicações específicas.
- Facebook - para proteger a conta Facebook do seu filho.
- Mensagens Instantâneas - para permitir ou bloquear chat com contactos específicos de mensagens instantâneas.

Os seguintes módulos podem ser acedidos para monitorizar a atividade do seu filho num dispositivo móvel:

- Localização - para descobrir a localização do dispositivo do seu filho no Google Maps.
- SMS - para bloquear mensagens de texto de determinado número.
- Chamadas - para bloquear chamadas de um número de telefone, tanto chamadas recebidas como chamadas efetuadas.

26.3.1. Controlo Web

O controlo Web ajuda-o a bloquear sites web com conteúdo inapropriado e definir restrições de tempo no acesso à Internet.

Para configurar o controlo Web para uma determinada conta de utilizador:

1. Clique em no painel **Web** para aceder à janela de **Atividade Web**.
2. Utilize o botão para ativar a **Atividade Web**.

Permitir ou bloquear um site Web

Utilize a janela **Atividade Web** para verificar todas as páginas Web visitadas pelo seu filho.

- Para bloquear o acesso a um site web, siga os seguintes passos:
  1. Clique no botão **Lista negra/Lista branca**.
  2. Insira o site web no respetivo campo.

3. Clique em **Bloquear** para adicionar o site Web à lista.
4. Se mudar de ideias, selecione o site Web e clique no botão **Remover** correspondente.

- Para permitir o acesso a um site Web bloqueado, siga estes passos:
  1. Clique no botão **Lista negra/Lista branca**.
  2. Insira o site web no respetivo campo.
  3. Clique em **Permitir** para adicionar o site Web à lista.
  4. Se mudar de ideias, selecione o site Web e clique no botão **Remover** correspondente.
- Para restringir o acesso à Internet a um site Web por tempo, siga estes passos:
  1. Aceda à janela Web da Lista negra/Lista branca, onde pode ver as páginas Web bloqueadas/permitidas.
  2. Em Permissão, clique em Bloqueado (ou Permitido) e selecione Agendar no menu suspenso.
  3. Selecione na grelha os intervalos de tempo durante os quais o acesso é permitido ou bloqueado. Pode clicar em células individuais, ou pode clicar e arrastar o rato para abranger períodos maiores.

     Clique no botão **Guardar**.

Controlo de Palavras-Chave

O Controlo por Palavra-chave ajuda-o a bloquear o acesso dos utilizadores a mensagens instantâneas, e a páginas web que contenham determinadas palavras. Ao usar o controlo por Palavra-chave, pode evitar que as crianças vejam palavras ou frases inapropriadas quando estão on-line. Além disso, pode certificar-se de que não irão fornecer a sua informação pessoal (como a morada ou o número de telefone) a pessoas que conheceram na Internet.

Para configurar o controlo por Palavra-chave para uma conta de utilizador específica, siga estes passos:

1. Clique no botão **Palavras-Chave**.
2. Insira a palavra-chave no respetivo campo.
3. Clique em **Bloquear** para adicionar a palavra à lista de palavras banidas. Se mudar de ideias, clique no correspondente botão **Remover**.

Filtro de Categoria

O filtro de categoria filtra o acesso aos sites web, de uma forma dinâmica, com base no respetivo conteúdo. Quando define a idade do seu filho, o filtro é automaticamente configurado para bloquear categorias de sites Internet considerados inadequados para a idade do seu filho. Esta configuração é adequada na maioria dos casos.

Se desejar maior controlo sobre o conteúdo da Internet a que os seus filhos estão expostos, pode escolher as categorias específicas do site Web que devem ser bloqueadas pelo Filtro de Categoria.

Para configurar em pormenor as definições do filtro de Categoria para uma conta específica de um utilizador, siga os seguintes passos:

1. Clique no botão **Categorias**.
2. Pode verificar que categorias web foram automaticamente bloqueadas/restringidas para a classe etária atualmente selecionada. Se não está satisfeito com as predefinições, pode configurar manualmente.
3. Clique em **Guardar**. Se mudar de ideias, clique no botão **Reiniciar** para utilizar o nível de proteção predefinido com base na idade do seu filho.

Restringir o acesso à Internet por tempo

Pode especificar quando o seu filho tem permissão para aceder à Internet utilizando a opção **Agendamento** na janela **Atividade Web**.

Para configurar em pormenor o acesso à Internet para uma conta específica de um utilizador, siga os seguintes passos:

1. Clique no botão **Agendar** .
2. Selecione na grelha os intervalos de tempo em que o acesso à Internet está bloqueado. Pode clicar em células individuais, ou pode clicar e arrastar o rato para abranger períodos maiores.
3. Clique no botão **Guardar**.

26.3.2. Controlo de Aplicações

O controlo de Aplicações permite que bloqueie a execução de qualquer aplicação. Jogos, software de multimédia e de mensagens, assim como outras categorias de software e malware podem ser bloqueados desta forma.

Para configurar o controlo de Aplicações para uma conta de utilizador específica, siga estes passos:

1. Clique no painél **Aplicações** para aceder à janela **Atividade Aplicações**.
2. Utilize o botão para ligar o **Controlo de Aplicações**.
3. Clique no botão **Lista Negra**.
4. Introduza o nome da aplicação:
   - Para bloquear uma aplicação num dispositivo móvel, selecione as aplicações que pretende bloquear na lista **Aplicações permitidas**.
   - Para bloquear uma aplicação no sistema operativo Windows, adicione o ficheiro executável da aplicação que pretende bloquear (.exe).
5. Clicar em **Bloquear** para adicionar a aplicação à lista de **Aplicações Bloqueadas** ou **Permitir** para adicionar a aplicação à lista de **Aplicações Permitidas**.

26.3.3. Proteção Facebook

O Controlo Parental monitoriza a conta Facebook do seu filho e reporta as principais atividades que estão a decorrer.

Estas atividades online são verificadas e é avisado se elas demonstram ser uma ameaça para a privacidade da sua conta.

Os elementos monitorizados da conta online incluem:

- o número de amigos
- comentários do seu filho ou dos seus amigos nas suas fotos ou posts
- mensagens
- Muro de posts
- vídeos e fotos uploaded
- definições de privacidade da conta

Para configurar a proteção Facebook para uma determinada conta de utilizador:

1. Clique em **Ligar ao perfil filho** no painél **Facebook**.
2. Para proteger a conta do seu filho no Facebook, instale a aplicação usando o link correspondente.

> **Nota**
> Para instalar a aplicação necessita das credenciais do perfil de Facebook do seu filho.

Para parar de monitorizar a conta do Facebook, utilize o botão **Desassociar conta** na parte superior.

26.3.4. Controlo de Mensagens Instantâneas

o controlo de Mensagens Instantâneas (MI) permite-lhe especificar os contactos de Mi do seu filho que lhe são permitidos fazer chat com, ou bloquear o acesso a mensagens instantâneas que contenham determinadas palavras.

> **Nota**
> O Controlo de Mensagens Instântaneas (MI) só está disponível para o Yahoo! Messenger e o Windows Live (MSN) Messenger.

Para configurar o controlo de Mensagens Instantâneas para uma conta de utilizador específica, siga estes passos:

1. Clique no painél **Mensagens Instantâneas** para aceder à janela **Atividade Mensagens Instantâneas**.
2. Utilize o botão para ligar a **Atividade de Mensagens Instantâneas**.

   Restringe o acesso das **mensagens Instantâneas** usando uma das opções disponíevis:

   - Botão **Lista negra** para introduzir o endereço de e-mail associado à ID de mensagem instantânea.
   - botão de **Palavras-chave** para bloquear o acesso a mensagens instantâneas que contém determinadas palavras.

26.3.5. Localização

Visualizar a localização atual do dispositivo no Google Maps. A localização é atualizada a cada 5 segundos para que possa controlá-lo se estiver em movimento.

A precisão da localização depende do quanto o Bitdefender é capaz de o determinar:

- Caso o GPS esteja ativado no dispositivo, a sua localização pode ser determinada no alcance de dois metros, desde que esteja ao alcance dos satélites GPS (ou seja, fora de um edifício).
- Se o dispositivo estiver dentro de um edifício, a sua localização pode ser determinada no alcance de 10 metros caso o Wi-Fi esteja ativado e existam rede sem fios disponíveis no seu alcance.
- Caso contrário, a localização será determinada utilizando apenas as informações da rede móvel, que pode oferecer uma precisão não melhor que várias centenas de metros.

Nota
Para que a **Localização** seja precisa, certifique-se de que ativou o GPS, o Wi-Fi ou a ligação à rede móvel no dispositivo móvel.

26.3.6. Controlo de mensagens de texto

O controlo de mensagens de texto ajuda a deixar de receber mensagens associadas a um número de telefone.

- Para bloquear mensagens de texto recebidas de um número de telefone, siga estes passos:
  1. Clique em no painel **SMS** para aceder à janela **Atividade SMS**.
  2. Utilize o botão para ativar a **Atividade SMS**.
  3. Clique no botão **Lista Negra**.
  4. Adicione um número de telefone no campo correspondente.
  5. Clique em **Bloquear** para adicionar o número de telefone à lista negra. O número de telefone será adicionado à lista de números de telefone bloqueados.
- Para permitir mensagens de texto um número de telefone bloqueado, siga estes passos:
  1. Clique no botão **Lista Negra** na parte superior.
  2. Selecione o número de telefone da lista.
  3. Clique em **Remover**. O número de telefone será removido da lista de números de telefone bloqueados.

Nota
Certifique-se que está a utilizar o indicativo específico quando inserir o número na lista.

26.3.7. Controlo de números de telefone

O controlo de número de telefone ajuda a deixar de efetuar ou receber chamadas associadas a um número de telefone.

- Para bloquear a realização ou recepção de chamadas associadas a um número de telefone, siga estes passos:

  1. Clique em no painel **Chamadas** para aceder à janela **Atividade de Chamadas**.
  2. Utilize o botão para ligar a **Atividade de Chamadas**.
  3. Clique no botão **Lista Negra**.
  4. Adicione um número de telefone no campo correspondente.
  5. Clique em **Bloquear** para adicionar o número de telefone à lista negra. O número de telefone será adicionado à lista de números de telefone bloqueados.

- Para permitir chamadas para um número de telefone bloqueado, siga estes passos:

  1. Clique no botão **Lista Negra** na parte superior.
  2. Selecione o número de telefone da lista.
  3. Clique em **Remover**. O número de telefone será removido da lista de números de telefone bloqueados.

Nota
Certifique-se que está a utilizar o indicativo específico quando inserir o número na lista.

27. PROTEÇÃO SAFEGO PARA O FACEBOOK

Você confia nos seus amigos online, mas pode confiar nos computadores deles? Utilize a proteção Safego para Facebook para proteger a sua conta e os seus amigos das ameaças online.

Safego é uma aplicação do Bitdefender desenvolvida para manter a sua conta do Facebook protegida. O seu papel é analisar as hiperligações que recebe dos seus amigos e monitorizar as suas definições de privacidade da conta.

Nota
A conta MyBitdefender é necessária para usar este recurso.
Para mais informação, por favor consulte o "*Conta MyBitdefender*" (p. 41).

Estas são as principais funcionalidades disponíveis para a sua conta Facebook:

- procura automaticamente nas publicações no seu Feed de Notícias hiperligações maliciosas.
- protege a sua conta contra ameaças online.

  Quando deteta uma publicação ou um comentário que sejam spam, pshishing ou malware, receberá uma mensagem de aviso.
- avisa os seus amigos sobre hiperligações suspeitas publicadas no Feed de Notícias.
- ajuda a construir uma rede segura de amigos que usam o recurso **Avaliação de amigos**.
- obtenha uma análise do estado da segurança do sistema pela Análise Rápida do Bitdefender.

Para aceder ao Safego para Facebook, siga estes passos:

- A partir da interface do Bitdefender:
  1. Abra a janela de Bitdefender.
  2. Aceda ao painel de **Ferramentas**.
  3. No módulo **Safego**, selecione **Ativar para o Facebook**.

     Será direccionado para a sua conta.

4. Use a sua informação de acesso ao Facebook para aceder à aplicação Safego.
5. Permitir que Safego aceda à sua conta Facebook.

Se o Safego já tiver sido ativado, poderá aceder às estatísticas da sua atividade ao selecionar **Relatórios para Facebook** no menu.

- Da conta MyBitdefender:
  1. Vá para: https://my.bitdefender.com.
  2. Inicie sessão na sua conta com o seu nome de utilizador e palavra-passe.
  3. Clique em **Proteção para Facebook**.

     Será exibida uma mensagem a informar que a proteção para Facebook não está ativada para a sua conta.
  4. Clique em **Ativar** para poder continuar.

     Será direccionado para a sua conta.
  5. Use a sua informação de acesso ao Facebook para aceder à aplicação Safego.
  6. Permitir que Safego aceda à sua conta Facebook.

28. BITDEFENDER USB IMMUNIZER

A funcionalidade Autorun inbuida no sistema operativo Windows é uma ferramenta bastante útil que permite aos computadores executarem automaticamente um ficheiro de um dispositivo de media ligado a ele. Por exemplo, as instalações de software podem iniciar automaticamente quando o CD é inserido na drive de CDs.

Infelizmente, esta funcionalidade também pode ser usada pelo malware para iniciar automaticamente e infiltrar no seu computador a partir de dispositivos media graváveis, tais como drives USB flash e cartões de memória ligados através de leitores de cartões. Numerosos ataques Autorun foram criados nestes últimos anos.

Com o Imunizador USB pode evitar que qualquer drive flash formatada em NTFS, FAT32 ou FAT jamais possa automaticamente executar malware. Uma vez que um dispositivo USB esteja imunizado, o malware já não o pode configurar para correr uma certa aplicação quando o dispositivo esteja ligado ao computador em Windows.

Para imunizar um dispositivo USB, siga estes passos:

1. Ligue a drive flash ao seu computador.
2. Explore o seu computador para localizar o dispositivo de armazenagem amovível e clique com o botão direito do rato sobre ele.
3. No menu contextual, aponte para o **Bitdefender** e selecione **Imunizar esta drive**.

> **Nota**
> Se a drive já foi imunizada, a mensagem **O dispositivo USB está protegido contra o malware baseado no autorun** aparecerá em vez da opção Imunizar.

Para prevenir que o seu computador execute malware de dispositivos USB não imunizados, desative a funcionalidade de media autorun. Para mais informação, por favor consulte o "*Usar monitorização de vulnerabilidade automática*" (p. 131).

29. GERIR OS SEUS COMPUTADORES REMOTAMENTE

A sua conta MyBitdefender permite-lhe gerir remotamente os produtos Bitdefender instalados nos seus computadores.

Use a MyBitdefender para criar e aplicar tarefas aos seus computadores a partir de um ponto remoto.

Qualquer computador será gerido a partir da conta MyBitdefender se cumprir com as seguintes condições:

- instalou o produto Bitdefender Internet Security 2015 no computador
- fez a ligação do produto Bitdefender à conta MyBitdefender.
- o computador está ligado à Internet

29.1. A aceder à MyBitdefender

O Bitdefender permite-lhe controlar a segurança dos seus computadores com o adicionar de tarefas aos seus produtos Bitdefender.

Com o Bitdefender pode aceder à sua conta MyBitdefender em qualquer computador ou dispositivo móvel ligado à Internet.

Aceder à MyBitdefender

- Em qualquer dispositivo com acesso à Internet:
  1. Abrir um browser web.
  2. Vá para:https://my.bitdefender.com
  3. Inicie sessão na sua conta com o seu nome de utilizador e palavra-passe.
- A partir do interface do Bitdefender :
  1. Abra a janela de Bitdefender.
  2. Clique no ícone na parte superior da janela e selecione **MyBitdefender** no menu suspenso.

29.2. Executar tarefas nos computadores

Para executar uma tarefa em um dos computadores, aceda à sua conta MyBitdefender.

Se clicar num ícone de um computador na parte de baixo da janela, pode ver todas as tarefas administrativas que pode levar a cabo no computador remoto.

Registo do produto
Permite-lhe registar o Bitdefender no computador remoto introduzindo a chave de licença.

Leva a cabo uma análise completa do seu PC
Permite-lhe executar uma análise completa num computador remoto.

Analisar áreas críticas para detetar malware ativo
Permite-lhe executar uma análise rápida num computador remoto.

Reparar incidências críticas
Permite-lhe reparar incidências que estão a afetar a segurança do seu computador remoto.

Atualização de Produto
Inicia o processo de atualização para o produto Bitdefender instalado neste computador.

OTIMIZAÇÃO DO SISTEMA

30. TUNEUP

O Bitdefender vem com um módulo TuneUp que irá ajudá-lo a manter a integridade do seu sistema. As ferramentas de manutenção oferecidas são criticas para o melhoramento do desempenho do seu sistema e para uma gestão eficiente do espaço do seu disco duro.

O Bitdefender fornece as seguintes ferramentas de otimização do PC:

- O Otimizador de Um Clique analisa e melhora a velocidade do seu sistema ao executar diversas tarefas com um único clique no botão.
- O Otimizador de Arranque reduz o tempo de arranque do seu sistema ao impedir que aplicações desnecessárias sejam executadas quando o PC for reiniciado.
- Limpeza do PC remove os ficheiros temporários da Internet e as cookies, os ficheiros não utilizados do sistema e os atalhos recentes dos documentos.
- Desfragmentador reorganiza os dados no disco rígido de forma a que as partes constituintes de cada ficheiro sejam armazenadas juntas e de forma contínua.
- Limpar Registo identifica e apaga referências orfãs ou inválidas do Registo do Windows. De forma a manter o Registo do Windows limpo e otimizado, é recomendável que execute o seu Limpa Registo uma vez por mês.
- O Restaurar Registo pode recuperar as chaves de registo previamente apagadas do Registo do Windows no uso do Limpa Registo Bitdefender.
- O Localizador de Duplicados encontra e apaga ficheiros que se encontram duplicados no seu sistema.

30.1. A otimizar a velocidade do seu sistema com apenas um clique

Problemas como falhas no disco rígido, restos de ficheiros de registo e o histórico do navegador, podem comprometer o desempenho do seu computador, e isso pode tornar-se irritante para si. Tudo isto pode ser corrigido com um único clique num botão.

O Otimizador de Um Clique permite-lhe identificar e remover ficheiros inúteis ao executar uma série de tarefas de limpeza ao mesmo tempo.

Para iniciar o processo Otimizador de Um Clique, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Ferramentas**.
3. No módulo **TuneUp**, selecione **Otimizador de Um Clique**. Para sair, clique em **Cancelar**.
   a. **A analisar**

      Aguarde que o Bitdefender termine de procurar por problemas no sistema.

      - Limpeza do Disco - identifica ficheiros antigos e inúteis do sistema.
      - Limpeza do Registo - identifica referências inválidas ou obsoletas no Registo do Windows.
      - Limpeza de Privacidade - identifica ficheiros temporários da Internet, cookies, cache e histórico do navegador.

      O número de problemas encontrados foi exibido. Recomenda-se revê-las antes de prosseguir com o procedimento de limpeza. Clique em **Otimizar** para continuar.

   b. **Otimização do sistema**

      Aguarde que o Bitdefender conclua a otimização do seu sistema.

   c. **Questões**

      Aqui pode ver o resultado da operação.

      Se desejar informações completas sobre o processo de otimização, clique na hiperligação **Visualizar relatório detalhado**.

30.2. A otimizar o tempo de arranque do seu PC.

O arranque prolongado do sistema é um problema real devido às aplicações que estão definidas para executar sem necessidade. Aguardar vários minutos para que um sistema arranque pode custar-lhe tempo precioso e produtividade.

A janela do Otimizador de Arranque apresenta quais aplicações estão a ser executadas durante o arranque do sistema e permite a gestão do seu comportamento nesta etapa.

Para iniciar o processo Otimizador de Arranque, siga esses passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Ferramentas**.
3. No módulo **TuneUp**, selecione **Otimizador de Arranque**.
   a. **Selecione as aplicações**

      Pode ver uma lista de aplicações que estão a executar no arranque do sistema. Selecione aquelas que quer desativar ou adiar durante o arranque.

   b. **Escolha da comunidade**

      Veja o que os outros utilizadores da Bitdefender decidiram fazer com a aplicação que selecionou. Com base na utilização do programa, três níveis são apresentados: **Alto**, **Médio** e **Baixo**.

   c. **Tempo de arranque do sistema**

      Verifique a barra de deslocamento na parte superior da janela para ver o tempo necessário tanto para o sistema como para as aplicações selecionadas para serem executadas durante o arranque.

      A reinicialização do sistema é necessária para ser capaz de obter as informações sobre o tempo de arranque do sistema e das aplicações.

   d. **Estado do arranque**

      - **Permitir.** Selecione esta opção quando quiser uma aplicação que execute no arranque do sistema. Esta opção é ativada por defeito.
      - **Atraso.**

        Selecione esta opção para adiar a execução de um programa no arranque do sistema. Isto significa que as aplicações selecionadas irão arrancar com um atraso de cinco minutos após o utilizador iniciar sessão no sistema.
        A funcionalidade do **Atraso** é pré-definida e não pode ser configurada pelo utilizador.
      - **Desativar.** Selecione esta opção para desativar a execução de um programa no arranque do sistema.

   e. **Resultados**

      As informações, como o tempo estimado para o arranque do sistema após adiar ou desativar programas, são apresentadas.

Pode ser necessária a reinicialização do sistema para ver todas as informações.

Clique em **OK** para guardar as alterações e fechar a janela.

Nota
Caso a sua subscrição expire ou decida desinstalar o Bitdefender, os programas que configurou para não serem executados no arranque serão restaurados para as suas predefinições de arranque.

30.3. Limpeza do seu PC

Cada vez que visita uma página web, são criados ficheiros temporários da Internet de forma a permitir que lhe aceda mais rapidamente da próxima vez.

Os cookies também são armazenados na seu computador quando visita uma página web.

O assistente de Limpeza do PC ajuda-o a libertar espaço em disco e a proteger a sua privacidade ao apagar ficheiros que já não são úteis.

- Cache dos browsers (Internet Explorer, Mozilla Firefox, Google Chrome).
- informações de depuração (ficheiros de relatório de erros, informações de memória e registos criados pelo Windows durante o seu funcionamento).
- Ficheiros desnecessários do Windows (reciclagem e ficheiros temporários do sistema).

Para iniciar o assistente de Limpeza do PC, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Ferramentas**.
3. No painel do **TuneUp**, selecione **Limpeza do PC**.
4. Siga o procedimento de três passos para efetuar a limpeza. Pode navegar pelo assistente utilizando o botão **Seguinte**. Para sair do assistente, clique em **Cancelar**.

   a. **Bem-vindo**

   Selecione **Típica** ou **Personalizada**. Em seguida, clique em **Seguinte** para continuar.

b. **Efetuar Limpeza**

c. **Resultados**

30.4. Desfragmentar volumes de discos rígidos

Quando copia um ficheiro que excede o tamanho do maior bloco de espaço livre no disco duro, a fragmentação do ficheiro ocorre. Porque não existe suficiente espaço livre para guardar o ficheiro de forma contínua, o mesmo é armazenado em diversos blocos. Quando o ficheiro framentado é acedido, os seus dados têm de ser lidos de diversos locais diferentes.

É recomendável que desfragmente o seu disco duro de forma a que:

- aceda mais rápido aos ficheiros.
- melhore o desempenho do sistema em geral.
- aumente o tempo de duração do seu disco duro.

Para iniciar o assistente do Desfragmentador do Disco, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Ferramentas**.
3. No painel **TuneUp**, selecione o **Desfragmentador de Disco**.
4. Siga o procedimento de cinco passos para efetuar a desfragmentação. Pode navegar pelo assistente utilizando o botão **Seguinte**. Para sair do assistente, clique em **Cancelar**.

   a. **Selecionar para análise**

      Selecione as partições que pretende analisar para fragmentação. Clique em **Continuar** para iniciar o processo de análise.

   b. **A analisar**

      Aguarde que o Bitdefender termine a análise das partições.

   c. **Selecionar para desfragmentação**

      É apresentado o estado de fragmentação das partições analisadas. Selecione as partições que pretende desfragmentar.

   d. **A desfragmentar**

      Aguarde que o Bitdefender termine a desfragmentação das partições.

   e. **Resultados**

Nota
A desfragmentação poderá demorar algum tempo uma vez que involve o mover de porções de dados armazenados de um lugar para o outro do disco duro. Recomendamos que execute a desfragmentação quando não está a usar o seu computador.

30.5. Limpar o registo do Windows

Muitas aplicações escrevem chaves no Registo do Windows durante a instalação. Quando remove tais aplicações, algumas das suas chaves de registo associadas poderão não ser apagadas e continuarem no seu Registo do Windows, tornando o seu sistema mais lento e até causando instabilidade no mesmo. O mesmo acontece quando apaga atalhos para ou determinados ficheiros das aplicações instaladas no seu sistema, como também no caso de drivers corrompidos.

Para iniciar o assistente do Limpador de Registo, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Ferramentas**.
3. No painel **TuneUp**, selecione **Limpeza de Registo**.
4. Siga o procedimento de quatro passos para limpar o registo. Pode navegar pelo assistente utilizando o botão **Seguinte**. Para sair do assistente, clique em **Cancelar**.
   a. **Bem-vindo**
   b. **Efetuar Análise**

      Aguarde que o Bitdefender termine a análise de registo.
   c. **Selecionar Chaves**

      Pode ver todas as chaves de registo inválidas ou orfãs detectadas. Informação detalhada é fornecida para cada chave de registo (nome, valor, prioridade, categoria).

      As chaves de registo estão agrupadas baseado na sua localização no Registo do Windows:

      - **Localizações do Software.** Chaves de registo que contêm informação sobre o caminho para as aplicações instaladas no seu computador.

        As chaves inválidas têm atribuídas uma baixa prioridade, o que significa que as pode apagar sem qualquer risco.

- **Controlos Pessoais.** Chaves de registo que contêm informação acerca das extensões dos ficheiros registados no seu computador. Estas chaves de registo são normalmente usadas para manter associações de ficheiros (para assegurar que o programa correto abre quando abre um ficheiro usando o Explorador do Windows). Por exemplo, tal chave de registo permite que o Windows abra um ficheiro .doc com o Microsoft Word.

  As chaves inválidas têm atribuídas uma baixa prioridade, o que significa que as pode apagar sem qualquer risco.

- **DLLs partilhadas.** As chaves de registo que contêm informação sobre a localização das DLLs (Dynamic Link Libraries) partilhadas. Funções de armazenagem DLLs que são usadas pelas aplicações instaladas para levar a cabo certas tarefas. Podem ser partilhadas por múltiplas aplicações para reduzir os requisitos de espaço em disco e em memória.

  Estas chaves de registo tornam-se inválidas quando a DLL que apontam é movida para outro local ou completamente removida (isto acontece quando desinstala um programa).

  As chaves inválidas têm atribuídas uma prioridade média, o que significa que apagá-las pode afetar negativamente o sistema.

Por defeito, todas as chaves estão marcadas para eliminação. Pode escolher eliminar individualmente as chaves inválidas de uma determinada categoria.

d. **Resultados**

30.6. Recuperar registo limpo

Por vezes, após limparmos o registo, poderá notar que o seu sistema não funciona bem ou que algumas aplicações não funcionam bem devido à falta de chaves no registo. Isto pode ser causado devido a chaves de registo partilhadas que foram apagadas durante a limpeza do registo ou por outras chaves apagadas. Para resolver este problema deverá recuperar o registo que foi limpo.

Para iniciar o assistente do Restauro de Registo, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Ferramentas**.

3. No painel **TuneUp**, selecione **Recuperação do Registo**.
4. Siga o procedimento de dois passos para recuperar o registo eliminado. Pode navegar pelo assistente utilizando o botão **Seguinte**. Para sair do assistente, clique em **Cancelar**.
   a. **Selecione checkpoint**

      Pode ver uma lista de pontos no tempo em que o Registo do Windows foi limpo. Clique na hiperligação **Visualizar Ficheiro** para verificar as chaves de registo detetadas. Selecione o ponto no tempo para restaurar o Registo do Windows.

      Atenção
      A recuperação da limpeza de registo pode sobrescrever as últimas chaves do registo que foram editadas desde a última limpeza do registo.

   b. **Resultados da tarefa**

30.7. Localizar ficheiros duplicados

Os ficheiros duplicados comem o seu espaço em disco. Imagine ter o mesmo ficheiro .mp3 aramazenado em três diferentes locais.

O assistente do Localizador de Duplicados ajuda a detetar e eliminar os ficheiros duplicados no seu computador.

Para iniciar o assistente do Localizador de Duplicados, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Ferramentas**.
3. No painel **TuneUp**, selecione **Localizador de Duplicados**.
4. Siga o procedimento de quatro passos para identificar e remover os duplicados. Pode navegar pelo assistente utilizando o botão **Seguinte**. Para sair do assistente, clique em **Cancelar**.
   a. **Selecionar alvo**

      Adicione as pastas onde procurar os ficheiros duplicados.

   b. **Procurar duplicados**

      Aguarde que o Bitdefender termine a procura de duplicados.

   c. **Ficheiros a eliminar**

Os ficheiros idênticos estão agrupados. Pode escolher uma ação a aplicar a todos os grupos ou a cada grupo isoladamente: manter mais recente, manter mais antigo, nenhuma ação. Também pode selecionar ações para ficheiros específicos.

Nota
Se não forem encontrados ficheiros duplicados, este passo será saltado.

d. **Resultados**

31. PERFIS

Atividades de trabalho diárias, ver filmes ou jogar podem provocar lentidão no sistema, especialmente se estes estiverem a ser executados simultaneamente com os processos de atualização do Windows e as tarefas de manutenção. Com o Bitdefender, pode agora escolher e aplicar o seu perfil preferido; o que irá ajustar o sistema a melhorar o desempenho de aplicações específicas.

O Bitdefender fornece os seguintes perfis:

- Perfil Trabalho
- Perfil de Filme
- Perfil de jogo

Caso decida não utilizar os **Perfis**, um perfil predefinido chamado **Padrão** será ativado e não fará qualquer otimização no seu sistema.

De acordo com a sua atividade, as seguintes definições do produto serão aplicadas quando um perfil é ativado:

- Todos os alertas e pop-ups do Bitdefender são desativados.
- A Atualização Automática é adiada.
- As análises agendadas são adiadas.
- O Consultor de Pesquisa é desativado.
- A Deteção de Invasão está configurada para o nível de proteção **Permissivo**.
- As ofertas especiais e as notificações do produto estão desativadas.

De acordo com a sua atividade, as seguintes definições do sistema são aplicadas quando um perfil é ativado:

- As Atualizações Automáticas do Windows são adiadas.
- Os alertas e pop-ups do Windows são desativados.
- Os programas desnecessários em segundo plano são suspensos.
- Os efeitos visuais são ajustados para o melhor desempenho.
- As tarefas de manutenção são adiadas.
- As definições do plano de energia são ajustadas.

31.1. Perfil Trabalho

A execução de várias tarefas no trabalho, tais como o envio de e-mails, ter uma videoconferência com os seus colegas distantes ou trabalhar com aplicações de design pode afetar o desempenho do sistema. O Perfil de Trabalho foi desenhado para ajudá-lo a melhorar a sua eficiência no trabalho, desativando alguns dos serviços e tarefas de manutenção em segundo plano.

A configurar o Perfil de Trabalho

Para configurar as ações a serem tomadas durante o Perfil de Trabalho, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Ferramentas**.
3. Clique no módulo de **Perfis**.
4. Na janela de **Definições do Perfil**, clique no botão **Configurar** na área do Perfil de Trabalho.
5. Escolha os ajustes do sistema que quer que sejam aplicados selecionando as seguintes opções:
   - Aumente o desempenho das aplicações de trabalho
   - Otimize as definições do produto para o perfil Trabalho
   - Adie programas em segundo plano e tarefas de manutenção
   - Adiar as Atualizações Automáticas do Windows
6. Clique em **Guardar** para guardar as alterações e fechar a janela.

A adicionar aplicações manualmente à lista do Perfil de Trabalho

Se o Bitdefender não entrar automaticamente no Perfil de Trabalho quando abre uma determinada aplicação de trabalho, pode adicionar a aplicação manualmente à **Lista de Aplicações**.

Para adicionar aplicações manualmente à Lista de aplicações do Perfil de Trabalho:

1. Abra a janela de Bitdefender.

2. Aceda ao painel de **Ferramentas**.
3. Clique no módulo de **Perfis**.
4. Na janela **Perfis**, clique no botão **Configurar** na área do perfil de Trabalho.
5. Na janela do **Perfil de Trabalho**, clique no link **Lista de aplicações**.
6. Clique em **Adicionar** para adicionar uma nova aplicação à **Lista de aplicações**.

   Uma nova janela irá aparecer. Vá até ao ficheiro executável da aplicação, selecione-o e clique em **OK** para o adicionar à lista.

31.2. Perfil de Filme

A exibição de conteúdo de vídeo de alta qualidade, como filmes de alta definição, exige recursos significativos do sistema. O Perfil de Filme ajusta as definições do sistema e do produto para que possa desfrutar de uma experiência cinematográfica agradável e sem interrupções.

A configurar o Perfil de Filme

Para configurar as ações a serem tomadas no Perfil de Filme:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Ferramentas**.
3. Clique no módulo de **Perfis**.
4. Na janela **Definições dos Perfis**, clique no botão **Configurar** na área do Perfil de Filme.
5. Escolha os ajustes do sistema que quer que sejam aplicados selecionando as seguintes opções:
   - Aumente o desempenho dos leitores de vídeo
   - Otimize as definições do produto para o perfil Filme
   - Adie programas em segundo plano e tarefas de manutenção
   - Adiar as Atualizações Automáticas do Windows
   - Ajuste o plano de energia e as definições visuais para filmes
6. Clique em **Guardar** para guardar as alterações e fechar a janela.

A adicionar manualmente leitores de vídeo à lista do Perfil de Filme

Se o Bitdefender não entrar automaticamente no Perfil de Filme ao iniciar uma determinada aplicação de reprodução de vídeo, pode adicionar manualmente a aplicação à **Lista de leitores**.

Para adicionar manualmente leitores de vídeo à Lista de leitores no Perfil de Filme:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Ferramentas**.
3. Clique no módulo de **Perfis**.
4. Na janela **Definições dos Perfis**, clique no botão **Configurar** na área de Perfil de Filme.
5. Na janela **Perfil de Filme**, clique no link **Lista de leitores**.
6. Clique em **Adicionar** para adicionar uma nova aplicação à **Lista de leitores**.

   Uma nova janela irá aparecer. Vá até ao ficheiro executável da aplicação, selecione-o e clique em **OK** para o adicionar à lista.

31.3. Perfil de jogo

Para desfrutar de uma experiência de jogo sem interrupções, é importante reduzir as interrupções do sistema e diminuir a lentidão. Ao utilizar heurísticas comportamentais, juntamente com uma lista de jogos conhecidos, o Bitdefender pode detectar automaticamente os jogos em execução e otimizar os recursos do sistema para que possa aproveitar a sua pausa de jogo.

A configurar o Perfil de Jogo

Para configurar as ações a serem tomadas durante o Perfil de Jogo, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Ferramentas**.
3. Clique no módulo de **Perfis**.

4. Na janela **Definições dos Perfis**, clique no botão **Configurar** na área do Perfil de Jogo.
5. Escolha os ajustes do sistema que quer que sejam aplicados selecionando as seguintes opções:
   - Aumente o desempenho dos jogos
   - Otimize as definições do produto para o perfil Jogo
   - Adie programas em segundo plano e tarefas de manutenção
   - Adiar as Atualizações Automáticas do Windows
   - Ajuste o plano de energia e as definições visuais para jogos
6. Clique em **Guardar** para guardar as alterações e fechar a janela.

Adicionar os jogos manualmente à lista de Jogos

Se o Bitdefender não entrar automaticamente no Perfil de Jogo ao iniciar um determinado jogo ou aplicação, pode adicionar a aplicação manualmente à **Lista de jogos**.

Para adicionar jogos manualmente à Lista de jogos no Perfil de Jogo:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Ferramentas**.
3. Clique no módulo de **Perfis**.
4. Na janela **Definições dos Perfis**, clique no botão **Configurar** na área do Perfil de Jogo.
5. Na janela **Perfil de Jogo**, clique no link **Lista de jogos**.
6. Clique em **Adicionar** para adicionar um novo jogo à **Lista de jogos**.

   Uma nova janela irá aparecer. Navegue até o ficheiro executável do jogo, selecione-o e clique em **OK** para adicioná-lo à lista.

31.4. Otimização em Tempo Real

A Otimização em Tempo Real do Bitdefender é um plug-in que melhora o desempenho do seu sistema de forma silenciosa, em segundo plano, garantindo que não é interrompido enquanto está num modo de perfil. Dependendo da carga do CPU, o plug-in monitoriza todos os processos,

focando naqueles que utilizam uma carga maior, para ajustá-los às suas necessidades.

Para ativar ou desativar a Otimização em Tempo Real, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Ferramentas**.
3. Clique no módulo de **Perfis**.
4. Na janela **Perfis**, selecione o separador **Definições de Perfis**.
5. Ative ou desative a Otimização em Tempo Real automática clicando no botão correspondente.

SOLUÇÃO DE PROBLEMAS

32. RESOLVER INCIDÊNCIAS COMUNS

Este capítulo apresenta alguns dos problemas que poderá encontrar ao utilizar o Bitdefender e as possíveis soluções. A maioria destes problemas pode ser resolvida com a configuração correta das definições do produto.

- "*O meu sistema parece estar lento*" (p. 190)
- "*A análise não inicia*" (p. 192)
- "*Já não consigo usar uma aplicação*" (p. 194)
- "*O que fazer quando o Bitdefender bloqueia um site Web ou uma aplicação online segura*" (p. 195)
- "*Como atualizar o Bitdefender numa ligação à Internet lenta*" (p. 201)
- "*O Meu Computador não está ligado à Internet. Como posso actualizar o Bitdefender?*" (p. 201)
- "*Os serviços Bitdefender não estão a responder*" (p. 202)
- "*O filtro Antispam não está a funcionar corretamente*" (p. 203)
- "*A funcionalidade Preenchimento automático na minha Carteira não funciona*" (p. 207)
- "*Remoção de Bitdefender falhou*" (p. 208)
- "*O meu sistema não reinicia após a instalação de Bitdefender*" (p. 210)

Se não conseguir encontrar o seu problema aqui, ou se as soluções apresentadas não resolvem o seu problema, pode contactar os representantes do apoio técnico da Bitdefender como mostrado no capítulo "*Pedir Ajuda*" (p. 227).

32.1. O meu sistema parece estar lento

Normalmente, após a instalação de um software de segurança, o sistema poderá abrandar ligeiramente, o que é, até um certo nível, normal.

Se notar um abrandamento significativo, este problema pode dever-se às seguintes razões:

- **O Bitdefender não é o único programa de segurança instalada no sistema.**

  Apesar de o Bitdefender procurar e remover os programas de segurança encontrados durante a instalação, é recomendado que remova todos os

outros programas antivírus utilizados antes de instalar o Bitdefender. Para mais informação, por favor consulte o "*Como posso remover outras soluções de segurança?*" (p. 83).

- **Não estão cumpridos os Requisitos Mínimos do Sistema para executar o Bitdefender.**

  Se o seu computador não cumprir os Requisitos Mínimos do Sistema, ficará lento, especialmente se estiver a executar muitas aplicações ao mesmo tempo. Para mais informação, por favor consulte o "*Requisitos mínimos do sistema*" (p. 3).

- **Há demasiadas chaves de registo inválidas no seu Registo do Windows.**

  A limpeza do Registo do Windows pode melhorar o desempenho do seu sistema. Para mais informação, por favor consulte o "*Limpar o registo do Windows*" (p. 179).

- **As unidades do seu disco rígido estão demasiado fragmentadas.**

  A fragmentação dos ficheiros abranda o acesso aos ficheiros e diminui o desempenho do sistema.

  A Desfragmentação do Disco pode melhorar o desempenho do seu sistema. Para mais informação, por favor consulte o "*Desfragmentar volumes de discos rígidos*" (p. 178).

  Para desfragmentar o seu disco com o sistema operativo do Windows, siga o caminho a partir do menu Iniciar: **Iniciar** → **Todos os Programas** → **Acessórios** → **Ferramentas do Sistema** → **Desfragmentador de Disco**.

- **Instalou aplicações que não utiliza**.

  Algum computador possui programas ou aplicações que não utiliza. E quaisquer programas indesejados são executados em segundo plano, ocupando espaço no disco rígido e na memória. Caso não utilize um programa, desinstale-o. Também se aplica a qualquer outro software pré-instalado ou aplicação de teste que se esqueceu de remover.

  > **Importante**
  > Caso suspeite que um programa ou aplicação seja parte essencial de seu sistema operativo, não remova o mesmo e entre em contacto com a Assistência ao Cliente do Bitdefender para obter assistência.

- **O seu sistema pode estar infetado**.

A velocidade do seu sistema e o seu comportamento geral também podem ser afectados pelo malware. Spyware, viruses, Trojans e adware prejudicam o desempenho do seu sistema. Certifique-se de que analisa o seu sistema periodicamente, pelo menos uma vez por semana. Recomendamos a utilização da Análise do Sistema do Bitdefender, pois a mesma analisa todos os tipos de malware que ameaçam a segurança do seu sistema.

Para iniciar a Análise do Sistema, siga estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. No módulo **Antivírus**, selecione a **Análise do Sistema**.
4. Siga os passos do assistente.

32.2. A análise não inicia

Este tipo de problema pode ter duas causas principais:

- **Uma instalação anterior do Bitdefender que não foi totalmente removida ou uma instalação do Bitdefender mal sucedida**.

  Neste caso, siga os seguintes passos:

  1. Remover o Bitdefender totalmente do sistema:
     - No **Windows XP**:
       a. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Adicionar/Remover Programas**.
       b. Encontre o **Bitdefender Internet Security 2015** e selecione **Remover**.
       c. Clique em **Remover** na janela que aparece e depois selecione **Eu quero reinstalá-lo**.
       d. Aguarde que o processo de desinstalação conclua e, em seguida, reinicie o sistema.
     - No **Windows Vista** e **Windows 7**:
       a. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.
       b. Encontre o **Bitdefender Internet Security 2015** e selecione **Desinstalar**.

c. Clique em **Remover** na janela que aparece e depois selecione **Eu quero reinstalá-lo**.

d. Aguarde que o processo de desinstalação conclua e, em seguida, reinicie o sistema.

- No **Windows 8**:

a. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.

b. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.

c. Encontre o **Bitdefender Internet Security 2015** e selecione **Desinstalar**.

d. Clique em **Remover** na janela que aparece e depois selecione **Eu quero reinstalá-lo**.

e. Aguarde que o processo de desinstalação conclua e, em seguida, reinicie o sistema.

2. Reinstale o seu produto Bitdefender

- **O Bitdefender não é a única solução de segurança instalada no seu sistema**.

Neste caso, siga os seguintes passos:

1. Remover a outra solução de segurança. Para mais informação, por favor consulte o "*Como posso remover outras soluções de segurança?*" (p. 83).
2. Remover o Bitdefender totalmente do sistema:

- No **Windows XP**:

a. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Adicionar/Remover Programas**.

b. Encontre o **Bitdefender Internet Security 2015** e selecione **Remover**.

c. Clique em **Remover** na janela que aparece e depois selecione **Eu quero reinstalá-lo**.

d. Aguarde que o processo de desinstalação conclua e, em seguida, reinicie o sistema.

- No **Windows Vista** e **Windows 7**:
  a. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.
  b. Encontre o **Bitdefender Internet Security 2015** e selecione **Desinstalar**.
  c. Clique em **Remover** na janela que aparece e depois selecione **Eu quero reinstalá-lo**.
  d. Aguarde que o processo de desinstalação conclua e, em seguida, reinicie o sistema.
- No **Windows 8**:
  a. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
  b. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.
  c. Encontre o **Bitdefender Internet Security 2015** e selecione **Desinstalar**.
  d. Clique em **Remover** na janela que aparece e depois selecione **Eu quero reinstalá-lo**.
  e. Aguarde que o processo de desinstalação conclua e, em seguida, reinicie o sistema.

3. Reinstale o seu produto Bitdefender

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 227).

32.3. Já não consigo usar uma aplicação

Este problema ocorre quando está a tentar utilizar um programa que estava a funcionar normalmente antes de instalar o Bitdefender.

Após instalar o Bitdefender pode deparar-se com uma das seguintes situações:

- Poderá receber uma mensagem do Bitdefender a informar que o programa está a tentar modificar o sistema.

- Pode receber uma mensagem de erro do programa que está a tentar utilizar.

Este tipo de situação ocorre quando o Controlo Ativo do Vírus deteta erroneamente algumas aplicações como maliciosas.

O Controlo Ativo de Vírus é um módulo do Bitdefender que monitoriza constantemente as aplicações executadas no seu sistema e denuncia o comportamento potencialmente malicioso. Como este recurso é baseado num sistema heurístico, poderá haver casos em que as aplicações legítimas são denunciadas pelo Controlo Ativo de Vírus.

Quando isto acontece, pode excluir a respetiva aplicação da monitorização do Controlo Ativo de Vírus.

Para adicionar o programa à lista de exceções, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Antivírus**.
4. Na janela **Antivírus**, selecione o separador **Exceções**.
5. Clique na hiperligação **Processos Excluídos**. Na janela que aparece, pode gerir as exceções do processo de Controlo Ativo de Vírus.
6. Adicionar exceções seguindo estes passos:
   a. Clique no botão **Adicionar** , localizado no cimo da tabela de exceções.
   b. Clique em **Explorar**, procure e selecione a aplicação que quer excluir e depois clique em **OK**.
   c. Manter a opção **Permitir** selecionada para evitar que o Controlo Ativo de Vírus bloqueie a aplicação.
   d. Prima **Adicionar**.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 227).

32.4. O que fazer quando o Bitdefender bloqueia um site Web ou uma aplicação online segura

O Bitdefender oferece uma experiência de navegação Web segura filtrando todo o tráfego da rede e bloqueando os conteúdos maliciosos. No entanto,

é possível que o Bitdefender considere um site Web ou uma aplicação online segura como insegura, o que fará com que a análise do tráfego de HTTP do Bitdefender bloqueie-os incorretamente.

Se a mesma página ou aplicação for bloqueada repetidamente, estes podem ser adicionados a uma lista branca para que não sejam analisados pelos mecanismos do Bitdefender, o qeu assegura uma experiência de navegação Web normal.

Para adicionar um site Web na **Lista branca**, sigas estes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Proteção da Internet**.
4. No separador **Definições**, clique na hiperligação **Lista branca**. Uma nova janela irá aparecer.
5. Forneça o endereço do site Web ou da aplicação online bloqueada no campo correspondente e clique em **Adicionar**.
6. Clique em **Guardar** para guardar as alterações e fechar a janela.

Apenas os sites Web e as aplicações em que confia totalmente devem ser adicionados a esta lista. Estes irão ser excluídos da análise pelos seguintes mecanismos: malware, phishing e fraude.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 227).

32.5. Não consigo ligar à Internet

Poderá verificar que um programa ou navegador da web já não consegue ligar à Internet ou aceder aos serviços em rede após a instalação do Bitdefender.

Neste caso, a melhor solução é configurar o Bitdefender para permitir automaticamente as ligações de e para a respetiva aplicação de software:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Firewall**.
4. Na janela da **Firewall**, selecione o separador **Regras**.

5. Para adicionar uma regra de aplicação, clique no botão **Adicionar regra**.
6. Uma nova janela irá aparecer onde poderá adicionar os detalhes. Certifique-se de que seleciona todos os tipos de rede disponíveis e na seção **Permissão** seleciona **Permitir**.

Feche o Bitdefender, abra a aplicação de software e tente de novo ligar-se à Internet.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 227).

32.6. Não consigo aceder a um dispositivo na minha rede

Dependendo da rede a que está ligado, a firewall do Bitdefender poderá bloquear a ligação entre o seu sistema e outro dispositivo (como outro computador ou uma impressora). Como resultado, já não poderá partilhar ou imprimir ficheiros.

Neste caso, a melhor solução é configurar o Bitdefender para permitir automaticamente as ligações de e para o respetivo dispositivo. Para cada ligação de rede pode configurar uma zona fidedigna e especial.

Uma zona fidefigna é um dispositivo em que confia totalmente. Todo o tráfego entre o seu computador e o dispositivo fiável é permitido. Para partilhar recursos com dispositivos específicos, tais como computadores ou impressoras, adicione-as como zonas fidedignas.

Para adicionar uma zona fidedigna à sua rede de adaptadores, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. Clique no módulo **Firewall**.
4. Na janela da **Firewall**, selecione o separador **Regras**.
5. Para adicionar uma zona, clique no botão **Adicionar regra**. Surgirá uma nova janela apresentando os endereços IP dos dispositivos ligados à rede.

6. Selecione o endereço IP do computador ou da impressora que deseja adicionar ou digite o endereço ou address range na caixa de texto providenciada.
7. No campo **Permissão** selecione **Permitir** e, em seguida, clique em **OK**.

Se ainda não conegue ligar-se ao dispositivo, a incidência poderá não ser causada pelo Bitdefender.

Procure por outras potenciais causas, tais como as seguintes:

- A firewall no outro computador poderá bloquear a partilha de ficheiros e impressoras com o seu computador.
  - Se a Firewall do Windows estiver a utilizada, pode ser configurada para permitir a partilha de ficheiros e impressora da seguinte forma:
    - No **Windows XP**:
      1. Clique em **Iniciar**, aceda ao **Painel de Controlo** e selecione **Centro de Segurança**.
      2. Abra a janela de definições da Firewall do Windows e selecione o separador **Exceções**.
      3. Selecione a caixa de verificação **Partilha de ficheiros e impressoras**.
    - No **Windows Vista e Windows 7**:
      1. Clique em **Iniciar**, aceda ao **Painel de Controlo** e selecione **Sistema e Segurança**.
      2. Aceda a **Firewall do Windows** e clique em **Permitir um programa através da Firewall do Windows**.
      3. Selecione a caixa de verificação **Partilha de ficheiros e impressoras**.
    - No **Windows 8**:
      1. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
      2. Clique em **Sistema e Segurança**, aceda a **Firewall do Windows** e selecione **Deixar uma aplicação passar pela Firewall do Windows**.
      3. Selecione a caixa de verificação **Partilha de ficheiros e impressoras** e clique em **OK**.

- Se outro programa de firewall estiver a ser utilizado, por favor consulte a documentação e ficheiro de ajuda.

- Condições gerais que podem impedir a utilização ou conexão com a impressora compartilhada:
  - Poderá precisar de se ligar com uma conta de administrador do Windows para aceder à impressora compartilhada.
  - As permissões são definidas para a impressora compartilhada para permitir acesso a um computador específico e apenas utilizadores. Se está a compartilhar a sua impressora, verifique as permissões definidas para a impressora para saber se o utilizador do outro computador está autorizado a aceder à impressora. Se está a tentar ligar-se a uma impressora compartilhada, verifique com o utilizador do outro computador se tem permissão para se conectar com a impressora.
  - A impressora ligada ao seu computador ou ao outro computador não está a ser compartilhada.
  - A impressora compartilhada não está adicionada ao computador.

  Nota
  Para aprender como gerir o compartilhamento de impressoras (compartilhar uma impressora, definir ou remover permissões para a impressora, conecta-se a uma rede de impressora ou a uma impressora partilhada), vá à Ajuda e Suporte do Windows (no menu Iniciar, clique em **Ajuda e Suporte**).

- O acesso a uma impressora em rede pode ser restringido a computadores ou apenas a utilizadores. Deverá verificar com o administrador da rede se tem ou não permissão para aceder à impressora.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 227).

32.7. A minha Internet está lenta

Esta situação poderá surgir depois de instalar o Bitdefender. Este problema poderá ser causado por erros na configuração da firewall do Bitdefender.

Para resolver esta situação, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.

3. Clique no módulo **Firewall**.
4. Na janela da **Firewall**, clique no botão para desativar a **Firewall**.
5. Verifique se a sua ligação à Internet melhorou com a firewall do Bitdefender desativada.
   - Se ainda tem uma ligação à Internet lenta, a incidência poderá não ser causada pelo Bitdefender. Deve contactar o seu Fornecedor de Serviço de Internet para confirmar se a ligação está operacional.

     Se receber a confirmação do seu Fornecedor de Serviços de Internet que a ligação está operacional e o problema persistir, contacte a Bitdefender como indicado na secção "*Pedir Ajuda*" (p. 227).
   - Se a ligação à Internet melhorou depois de desativar a firewall do Bitdefender, siga os seguintes passos:
     a. Abra a janela de Bitdefender.
     b. Aceda ao painel de **Proteção**.
     c. Clique no módulo **Firewall**.
     d. Na janela da **Firewall**, selecione o separador **Definições**.
     e. Ir para **Bloquear partilha de ligação à Internet** e clique no botão para ativá-lo.
     f. Vá a **Bloquear análise de portas na rede** e clique no botão para ativá-lo.
     g. Aceda ao separador **Adaptadores** e selecione a sua ligação à Internet.
     h. Na coluna **Tipo de Rede** selecione **Casa/Trabalho**.
     i. Na coluna **Modo Escondido** selecione **Remoto**. Configure a coluna **Genérico** como **Ativado**
     j. Feche o Bitdefender, reinicie o sistema e verifique a velocidade de ligação à Internet.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 227).

32.8. Como atualizar o Bitdefender numa ligação à Internet lenta

Se tiver uma ligação à Internet lenta (por exemplo, ligação telefónica), poderão ocorrer erros durante o processo de atualização.

Para manter o seu sistema atualizado com as mais recentes assinaturas de malware Bitdefender, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Clique no ícone na parte superior da janela e selecione **Definições Gerais** do menu suspenso.
3. Na janela de **Definições Gerais**, selecione o separador **Atualizar**.
4. Ao lado do **Atualizar as regras de processamento**, selecione **Exibir antes de transferir** do menu suspenso.
5. Volte à janela principal e clique no botão de ação **Atualizar** à direita na janela.
6. Selecione apenas **Atualizações das assinaturas** e clique em **OK**.
7. O Bitdefender vai transferir e instalar apenas as atualizações das assinaturas de malware.

32.9. O Meu Computador não está ligado à Internet. Como posso actualizar o Bitdefender?

Se o seu computador não estiver ligado à Internet, tem de transferir manualmente as atualizações para um computador com acesso à Internet e, depois, transferi-las para o seu computador com um dispositivo amovível, por exemplo, um USB.

Siga os seguintes passos:

1. Num computador com acesso à Internet, abra o navegador da Internet e vá a:

   http://www.bitdefender.pt/site/view/Desktop-Products-Updates.html

2. Na coluna **Atualização Manual**, clique na hiperligação que corresponde ao seu produto e à arquitectura do sistema. Se não sabe se a versão do seu Windows é de 32 ou 64 bits, consulte "*Estou a utilizar uma versão de 32 ou 64 Bit do Windows?*" (p. 81).

3. Guarde o ficheiro com o nome weekly.exe no sistema.
4. Mova o ficheiro transferido para um dispositivo amovível, tal como uma unidade USB, e depois para o seu computador.
5. Faça duplo clique no ficheiro e siga os passos do assistente.

32.10. Os serviços Bitdefender não estão a responder

Este artigo ajuda-o a troubleshoot os erros de**Os Serviços Bitdefender não estão a responder**. Pode encontrar esse erro da seguinte forma:

- O ícone Bitdefender na Barra de Notificação está a cinzento e é informado que os serviços do Bitdefender não estão a responder.
- A janela do Bitdefender indica que os serviços do Bitdefender não estão a responder.

O erro pode ter ocorrido devido a um dos seguintes fatores:

- problemas temporários de comunicação entre os serviços da Bitdefender.
- alguns dos serviços da Bitdefender estão parados.
- Outras soluções de segurança em execução no seu computador, ao mesmo tempo que o Bitdefender.

Para solucionar este erro, tente estas soluções:

1. Espere uns momentos e verifique se existe alguma alteração. Este erro pode ser temporário.
2. Reinicie o computador e aguarde alguns momentos até o Bitdefender iniciar. Abra o Bitdefender e veja se o erro se mantém. Reiniciar o computador normalmente resolve o problema.
3. Verifique se tem qualquer outra solução de segurança instalada na medida em que possam interferir no funcionamento normal do Bitdefender. Se for este o caso, recomendamos que remova todas as outras soluções de segurança e reinstale Bitdefender.

   Para mais informação, por favor consulte o "*Como posso remover outras soluções de segurança?*" (p. 83).

Se o erro persistir, por favor contacte os nossos representantes do suporte conforme descrito na secção "*Pedir Ajuda*" (p. 227).

32.11. O filtro Antispam não está a funcionar corretamente

Este artigo ajuda a solucionar os seguintes problemas relacionados com a operação de filtragem do Antispam do Bitdefender:

- Um número de mensagens de e-mail legítimas são marcadas como [spam].
- Muitas mensagens spam não estão marcadas de acordo com o filtro antispam.
- O filtro antispam não deteta qualquer mensagem de spam.

32.11.1. Mensagens legítimas são marcadas como [spam]

Mensagens legítimas são marcadas como [spam] simplesmente porque elas parecem spam para o filtro antispam do Bitdefender. Pode normalmente resolver este problema ao configurar adequadamente o filtro Antispam.

O Bitdefender adiciona automaticamente os remetentes das suas mensagens de e-mail à Lista de Amigos. As mensagens de e-mail recebidas dos contactos na lista de Amigos são consideradas legítimas. Elas não são verificadas pelo filtro antispam e, deste modo, elas nunca são marcadas como [spam].

A configuração automática da lista de Amigos não impede a deteção de erros que podem ocorrer nestas situações:

- Recebeu muitos e-mails publicitários solicitados como resultado de se inscrever em vários sites. Neste caso, a solução é adicionar à Lista de Amigos o endereço de e-mail do qual recebeu esses e-mails.
- Uma parte significativa dos seus mails legítimos são de pessoas com quem nunca trocou e-mails antes, tais como clientes, potenciais parceiros empresariais e outros. Outras soluções são requeridas neste caso.

  Se estiver a utilizar um cliente de email com o qual o Bitdefender é compatível, indique erros de deteção.

> **Nota**
> O BiDefender integra uma barra antispam de facil utilização, nos clientes de email mais comuns. Para ver a lista completa de clientes de e-mail suportados, por favor consulte o "*Clientes de email e protocolos suportados*" (p. 114).

Adicionar contactos à Lista de Amigos

Se está a utilizar um cliente de mail suportado, pode facilmente adicionar os remetentes das mensagens legítimas à lista de Amigos. Siga os seguintes passos:

1. No seu cliente de mail, selecione a mensagem de e-mail do remetente que quer adicionar à lista de Amigos.
2. Clique no botão **Adicionar Amigos** da barra de tarefas antispam do Bitdefender.
3. Poderá ser convidado a reconhecer os endereços adicionados à lista de Amigos. Selecione **Não mostrar esta mensagem outra vez** e clique **OK**.

Irá sempre receber mensagens de e-mail destes endereços, independentemente do conteúdo da mensagem.

Se está a utilizar um cliente de mail diferente, poderá adicionar os contactos à lista Amigos a partir do interface do Bitdefender. Siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. No módulo **Antispam**, selecione **Gerir Amigos**.

   A janela de configuração irá aparecer.
4. Digite o endereço de email onde quer sempre receber as mensagens de email e depois clique em **Adicionar**. Pode adicionar quantos endereços de email desejar.
5. Clique em **OK** para guardar as alterações e fechar a janela.

Indique os erros de deteção

Se estiver a usar um cliente de e-mail suportado, pode facilmente corrigir o filtro antispam (indicando mensagens de correio eletrónico que não deveriam ter sido marcadas como[spam]). Se o fizer, ajuda a melhorar a eficiência do filtro antispam. Siga os seguintes passos:

1. Abra o mail de cliente.
2. Vá à pasta de lixo eletrónico, para onde são movidas as mensagens.
3. Selecione a mensagem legítima incorretamente marcada como [spam] pelo Bitdefender.

4. Clique no botão **Adicionar Amigos** da barra de tarefas antispam do Bitdefender para adicionar o remetente à lista de Amigos. Pode necessitar de clicar em **OK** para confirmar. Irá sempre receber mensagens de e-mail destes endereços, independentemente do conteúdo da mensagem.
5. Clique no botão **Não Spam** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela de mail do cliente). A mensagem de email será movida para a pasta de Entrada.

32.11.2. Muitas mensagens de spam não são detetadas

Se está a receber muitas mensagens spam que não estão marcadas como [spam], tem de configurar o filtro antispam Bitdefender de modo a melhorar a sua eficiência.

Tente as seguintes soluções:

1. Se estiver a utilizar um cliente de email com o qual o Bitdefender é compatível, indique mensagens de spam não detetadas.

   Nota

   O BiDefender integra uma barra antispam de facil utilização, nos clientes de email mais comuns. Para ver a lista completa de clientes de e-mail suportados, por favor consulte o "*Clientes de email e protocolos suportados*" (p. 114).

2. Adicione spammers à lista de Spammers. As mensagens de e-mail recebidas dos endereços na lista de Spammers são automaticamente marcadas como [spam].

Indica mensagens de spam não detetadas

Se estiver a utilizar um cliente de e-mail suportado, pode facilmente indicar quais as mensagens de e-mail que devem ser detectadas como spam. Se o fizer, ajuda a melhorar a eficiência do filtro antispam. Siga os seguintes passos:

1. Abra o mail de cliente.
2. Vá à pasta Caixa de Entrada.
3. Selecione as mensagens spam não detetadas

4. Clique no botão **É Spam** na barra de ferramentas antispam do Bitdefender (normalmente localizada na parte superior da janela de email do cliente). São imediatamente marcadas como [spam] e movidas para a pasta de lixo electrónico.

Adicionar spammers à lista de Spammers

Se está a utilizar um cliente de mail suportado, pode facilmente adicionar os remetentes das mensagens spam à lista Spammers. Siga os seguintes passos:

1. Abra o mail de cliente.
2. Vá à pasta de lixo eletrónico, para onde são movidas as mensagens.
3. Selecione a mensagem marcada como [spam] pelo Bitdefender.
4. Clique no botão **Adicionar Spammer** da barra de tarefas antispam do Bitdefender.
5. Poderá ser convidado a reconhecer os endereços como Spammers. Selecione **Não mostrar esta mensagem outra vez** e clique **OK**.

Se está a utilizar um cliente de mail diferente, poderá adicionar manualmente os spammers à lista de Spammers a partir do interface do Bitdefender. É conveniente que o faça apenas quando receber várias mensagens spam do mesmo endereço e-mail. Siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. No módulo **Antispam**, selecione **Gerir Spammers**.

   A janela de configuração irá aparecer.
4. Digite o endereço de email do spammer e depois clique em **Adicionar**. Pode adicionar quantos endereços de email desejar.
5. Clique em **OK** para guardar as alterações e fechar a janela.

32.11.3. O Filtro Antispam não deteta nenhuma mensagem spam

Se nenhuma mensagem spam for marcada como [spam], poderá haver algum problema como o filtro Antispam do Bitdefender. Antes de resolver este

problema, certifique-se de que não é causado por nenhuma das seguintes condições:

- A proteção antispam poderá estar desligada. Para verificar o estado da proteção antispam, abra a janela do Bitdefender, aceda ao painel **Proteção**, clique no módulo **Antispam** e verifique o botão na janela de **Definições**.

  Se o Antispam estava desligado, era isso que estava a causar o problema. Clique no botão para ligar a proteção antispam.

- A proteção de Antispam do Bitdefender está disponível apenas para clientes de correio eletrónico configurado para receber mensagens de e-mail via protocolo POP3. Isto significa o seguinte:

  - As mensagens de Email obtidas através de Webmail (Yahoo, Gmail, Hotmail ou outros) não são filtradas como spam pelo Bitdefender.
  - Se o seu cliente de e-mail está configurado para receber mensagens de e-mail usando outro protocolo que não o POP3 (por exemplo, IMAP4), o filtro Antispam do Bitdefender não as analisará à procura de spam.

  Nota

  POP3 é um dos protocolos mais utilizados para fazer o download de mensagens de e-mail a partir de um servidor de correio. Se você não sabe o protocolo que o seu cliente de e-mail utiliza para importar mensagens de e-mail, solicite à pessoa que o configurou.

- O Bitdefender Internet Security 2015 não analisa o tráfego POP3 do Lotus Notes.

Uma solução possivel é reparar ou reinstalar o produto. Contudo, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 227).

32.12. A funcionalidade Preenchimento automático na minha Carteira não funciona

Guardou as suas credenciais online na Carteira do Bitdefender e constatou que o preenchimento automático não está a funcionar. Normalmente, este problema surge quando a extensão da Carteira do Bitdefender não está instalada no seu browser.

Para resolver esta situação, siga estes passos:

- No **Internet Explorer:**
  1. Abra o Internet Explorer.
  2. Clique em Ferramentas.
  3. Clique em Gerir suplementos.
  4. Clique em Ferramentas e Extensões.
  5. Aponte para **Carteira do Bitdefender** e clique em Ativar.
- No **Mozilla Firefox:**
  1. Abra o Mozilla Firefox.
  2. Clique em Ferramentas.
  3. Clique em Suplementos.
  4. Clique em Extensões.
  5. Aponte para **Carteira do Bitdefender** e clique em Ativar.
- No **Google Chrome:**
  1. Abra o Google Chrome.
  2. Aceda ao ícone Menu.
  3. Clique em Definições.
  4. Clique em Extensões.
  5. Aponte para **Carteira do Bitdefender** e clique em Ativar.

Nota
O suplemento será ativado após reiniciar o browser.

Agora verifique se a funcionalidade de preenchimento automático na Carteira está a funcionar para as suas contas online.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 227).

32.13. Remoção de Bitdefender falhou

Caso pretenda remover o seu produto Bitdefender e constate que o processo demora ou o sistema bloqueia, clique em **Cancelar** para interromper a ação. Se isso não funcionar, reinicie o sistema.

Se a remoção falhar, algumas chaves de registo e ficheiros do Bitdefender poderão permanecer no seu sistema. Esses resquícios podem impedir uma nova instalação do Bitdefender. Podem também afectar o desempenho e a estabilidade do sistema.

Para remover completamente Bitdefender do seu sistema, siga estes passos:

- No **Windows XP**:
  1. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Adicionar/Remover Programas**.
  2. Encontre o **Bitdefender Internet Security 2015** e selecione **Remover**.
  3. Clique em **Remover** na janela que aparece.
  4. Neste passo tem as seguintes opções:
     - **Eu quero reinstalá-lo** - irá remover completamente o Bitdefender. O Verificador de Vírus em 60 segundos do Bitdefender não será instalado.
     - **Eu quero removê-lo permanentemente** - irá remover completamente o Bitdefender. O Verificador de Vírus em 60 segundos do Bitdefender será instalado no seu sistema para o proteger contra malware.

     Selecione a opção pretendida e clique em **Seguinte**.
  5. Aguarde que o processo de desinstalação conclua e, em seguida, reinicie o sistema.
- No **Windows Vista** e **Windows 7**:
  1. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.
  2. Encontre o **Bitdefender Internet Security 2015** e selecione **Desinstalar**.
  3. Clique em **Remover** na janela que aparece.
  4. Neste passo tem as seguintes opções:
     - **Eu quero reinstalá-lo** - irá remover completamente o Bitdefender. O Verificador de Vírus em 60 segundos do Bitdefender não será instalado.
     - **Eu quero removê-lo permanentemente** - irá remover completamente o Bitdefender. O Verificador de Vírus em 60 segundos do Bitdefender será instalado no seu sistema para o proteger contra malware.

Selecione a opção pretendida e clique em **Seguinte**.

5. Aguarde que o processo de desinstalação conclua e, em seguida, reinicie o sistema.

- No **Windows 8**:

1. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
2. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.
3. Encontre o **Bitdefender Internet Security 2015** e selecione **Desinstalar**.
4. Clique em **Remover** na janela que aparece.
5. Neste passo tem as seguintes opções:

   - **Eu quero reinstalá-lo** - irá remover completamente o Bitdefender. O Verificador de Vírus em 60 segundos do Bitdefender não será instalado.
   - **Eu quero removê-lo permanentemente** - irá remover completamente o Bitdefender. O Verificador de Vírus em 60 segundos do Bitdefender será instalado no seu sistema para o proteger contra malware.

   Selecione a opção pretendida e clique em **Seguinte**.

6. Aguarde que o processo de desinstalação conclua e, em seguida, reinicie o sistema.

Nota

O Verificador de Vírus em 60 segundos do Bitdefender é uma aplicação livre que utiliza a tecnologia de análise na nuvem para detetar programas maliciosos e ameaças em menos de 60 segundos.

32.14. O meu sistema não reinicia após a instalação de Bitdefender

Se instalou o Bitdefender e não consegue reiniciar o seu sistema no modo normal, podem existir vários motivos para este problema.

Isto é muito provavelmente causado por uma instalação anterior de Bitdefender que não foi removida adequadamente ou por outra solução de segurança que ainda se encontra no sistema.

Eis como pode resolver cada situação:

- **Você tinha o Bitdefender anteriormente e não o removeu corretamente.**

  Para resolver isto, siga estes passos:

  1. Reinicie o seu sistema e inicie sessão no Modo de Segurança. Para saber como fazer isto, consulte "*Como posso reiniciar no Modo de Segurança?*" (p. 85).
  2. Remove Bitdefender do seu sistema:
     - No **Windows XP**:
       a. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Adicionar/Remover Programas**.
       b. Encontre o **Bitdefender Internet Security 2015** e selecione **Remover**.
       c. Clique em **Remover** na janela que aparece e depois selecione **Eu quero reinstalá-lo**.
       d. Clique em **Seguinte** para continuar.
       e. Desmarque a opção **Instalar o Verificador de Vírus em 60 segundos do Bitdefender** e clique em **Seguinte**.
       f. Aguarde até que o processo de desinstalação seja concluído.
       g. Reinicie o sistema no modo normal.
     - No **Windows Vista** e **Windows 7**:
       a. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.
       b. Encontre o **Bitdefender Internet Security 2015** e selecione **Desinstalar**.
       c. Clique em **Remover** na janela que aparece e depois selecione **Eu quero reinstalá-lo**.
       d. Clique em **Seguinte** para continuar.
       e. Desmarque a opção **Instalar o Verificador de Vírus em 60 segundos do Bitdefender** e clique em **Seguinte**.
       f. Aguarde até que o processo de desinstalação seja concluído.
       g. Reinicie o sistema no modo normal.
     - No **Windows 8**:

a. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.

b. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.

c. Encontre o **Bitdefender Internet Security 2015** e selecione **Desinstalar**.

d. Clique em **Remover** na janela que aparece e depois selecione **Eu quero reinstalá-lo**.

e. Clique em **Seguinte** para continuar.

f. Desmarque a opção **Instalar o Verificador de Vírus em 60 segundos do Bitdefender** e clique em **Seguinte**.

g. Aguarde até que o processo de desinstalação seja concluído.

h. Reinicie o sistema no modo normal.

3. Reinstale o seu produto Bitdefender

- **Você tinha uma solução de segurança diferente anteriormente e não a eliminou corretamente.**

  Para resolver isto, siga estes passos:

  1. Reinicie o seu sistema e inicie sessão no Modo de Segurança. Para saber como fazer isto, consulte "*Como posso reiniciar no Modo de Segurança?*" (p. 85).
  2. Remova as outras soluções de segurança do seu sistema:
     - No **Windows XP**:
       a. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Adicionar/Remover Programas**.
       b. Aguarde alguns momentos até que a lista do software instalado seja apresentada.
       c. Encontre o nome do programa que pretende remover e selecione **Remover**.
       d. Aguarde que o processo de desinstalação conclua e, em seguida, reinicie o sistema.
     - No **Windows Vista** e **Windows 7**:

a. Clique em **Iniciar**, vá ao **Painel de Controlo** e faça duplo clique sobre **Programas e Recursos**.

b. Aguarde alguns momentos até que a lista do software instalado seja apresentada.

c. Encontre o nome do programa que pretende remover e selecione **Remover**.

d. Aguarde que o processo de desinstalação conclua e, em seguida, reinicie o sistema.

- No **Windows 8**:

a. A partir do ecrã Iniciar do Windows, localize **Painel de Controlo** (por exemplo, pode começar a digitar "Painel de Controlo" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.

b. Clique em **Desinstalar um programa** ou **Programas e Funcionalidades**.

c. Aguarde alguns momentos até que a lista do software instalado seja apresentada.

d. Encontre o nome do programa que pretende remover e selecione **Remover**.

e. Aguarde que o processo de desinstalação conclua e, em seguida, reinicie o sistema.

Para desinstalar corretamente outro software, aceda ao site Web do fornecedor e execute a ferramenta de desinstalação ou contacte-o para diretamente, para que lhe indiquem os procedimentos de desinstalação.

3. Reinicie o seu sistema no modo normal e reinstale o Bitdefender.

Já seguiu os passos acima e o problema não está resolvido.

Para resolver isto, siga estes passos:

1. Reinicie o seu sistema e inicie sessão no Modo de Segurança. Para saber como fazer isto, consulte "*Como posso reiniciar no Modo de Segurança?*" (p. 85).
2. Usar a opção de Restauro do Sistema do Windows para restaurar o computador para uma data anterior antes de instalar o produto Bitdefender. Para saber como fazer isto, consulte "*Como posso usar o Restauro do Sistema no Windows?*" (p. 84).

3. Reinicie o sistema no modo normal e contacte os nossos representantes do suporte conforme descrito na secção "*Pedir Ajuda*" (p. 227).

33. REMOVER MALWARE DO SEU SISTEMA

O malware pode afetar o seu sistema de várias formas e a atuação do Bitdefender depende do tipo de ataque por malware. Como os vírus alteram frequentemente o modo de ação, é difícil estabelecer um padrão com base no comportamento e nas ações.

Há situações em que o Bitdefender não consegue remover automaticamente a infecção por malware do seu sistema. Nestes casos, a sua intervenção é necessária.

- "*Modo de Recuperação Bitdefender*" (p. 215)
- "*O que fazer se o Bitdefender encontrar vírus no seu computador?*" (p. 218)
- "*Como posso limpar um vírus num ficheiro?*" (p. 219)
- "*Como posso limpar um vírus num ficheiro do email?*" (p. 220)
- "*O que fazer se suspeitar que um ficheiro é perigoso?*" (p. 221)
- "*Como limpar ficheiros infectados da Informação de Volume do Sistema*" (p. 222)
- "*O que são os ficheiros protegidos por palavra-passe no relatório de análise?*" (p. 224)
- "*O que são os itens ignorados no relatório de análise?*" (p. 224)
- "*O que são os ficheiros muito comprimidos no relatório de análise?*" (p. 224)
- "*Por que é que Bitdefender eliminou automaticamente um ficheiro infectado?*" (p. 225)

Se não conseguir encontrar o seu problema aqui, ou se as soluções apresentadas não resolvem o seu problema, pode contactar os representantes do apoio técnico da Bitdefender como mostrado no capítulo "*Pedir Ajuda*" (p. 227).

33.1. Modo de Recuperação Bitdefender

Modo do Recuperação é uma característica do Bitdefender que lhe permite analisar e desinfectar todas as partições do disco rígido existentes fora do seu sistema operativo.

Depois de instalar o Bitdefender Internet Security 2015, o Modo de Recuperação pode ser usado mesmo que já não consiga arrancar no Windows.

Iniciar o seu sistema no Modo de Recuperação

Pode entrar no Modo de Recuperação de duas formas:

A partir da janela do Bitdefender

Para entrar no Modo de Recuperação diretamente a partir do Bitdefender, siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Aceda ao painel de **Proteção**.
3. No módulo **Antivírus**, selecione **Modo de Recuperação**.

   A janela de confirmação irá aparecer. Clique **Sim** para reiniciar o seu computador.
4. Depois do computador reiniciar, aparecerá um menu que o notifica para escolher um sistema operativo. Escolha **Modo de Recuperação do Bitdefender** e prima **Enter** para iniciar no ambiente do Bitdefender, de onde pode limpar a sua partição do Windows.
5. Se notificado, prima **Enter** e selecione a resolução do ecrã mais aproximada daquela que normalmente usa. Depois prima de novo **Enter**.

   O Modo de Recuperação do Bitdefender irá carregar dentro de momentos.

Arranque o seu computador diretamente no Modo de Recuperação

Se o Windows já não iniciar, pode arrancar o seu computador diretamente no Modo de Recuperação do Bitdefender, seguindo os passos abaixo:

> **Nota**
> Este método não se encontra disponível em computadores com Windows XP.

1. Inicie / reinicie o seu computador e comece a premir a tecla **espaços** do seu teclado antes de aparecer o logo do Windows.
2. Um menu surge notificando-o para selecionar um sistema operativo para iniciar. Prima **TAB** para ir para a área das ferramentas. Escolha

Imagem de Recuperação Bitdefender e prima a tecla **Enter** arrancar num ambiente do Bitdefender

3. Se notificado, prima **Enter** e selecione a resolução do ecrã mais aproximada daquela que normalmente usa. Depois prima de novo **Enter**.

   O Modo de Recuperação do Bitdefender irá carregar dentro de momentos.

Analisar o seu sistema no Modo de Recuperação

Para analisar o seu sistema no Modo de Recuperação, siga os seguintes passos:

1. Entre no Modo de Recuperação, conforme descrito em "Iniciar o seu sistema no Modo de Recuperação" (p. 216).
2. O logo do Bitdefender surgirá e os motores antivírus começarão a ser copiados.
3. Uma janela de boas-vindas aparece. Clique em **Continuar**.
4. Iniciou-se uma atualização de assinaturas antivirus.
5. Quando a atualização estiver concluída, a janela da Análise-a-pedido do Bitdefender surgirá.
6. Clique em **Analisar Agora**, selecione o alvo da análise na janela que surge e clique em **Abrir** para iniciar a análise.

   Recomenda-se que analise toda a partição do Windows.

   > **Nota**
   > Ao trabalhar no Modo de Recuperação, lida com nomes de partições do tipo do Linux. As partições do disco surgirão como sda1 provavelmente correspondendo à (C:) partição do Windows, sda2 correspondendo a (D:) e assim sucessivamente.

7. Aguarde que a análise termine. Se for detectado algum malware, siga as instruções para remover a ameaça.
8. Para sair do Modo de Recuperação, clique com o botão direito do rato numa área vazia do ambiente de trabalho, selecione **Sair** no menu que aparece e depois escolha entre reiniciar ou encerrar o computador.

33.2. O que fazer se o Bitdefender encontrar vírus no seu computador?

Pode verificar se há um vírus no seu computador de uma das seguintes formas:

- O Bitdefender analisou o seu computador e encontrou itens infectados.
- Um alerta de vírus avisa que o Bitdefender bloqueou um ou vários vírus no seu computador.

Nestas situações, atualize o Bitdefender para se certificar que possui as assinaturas de malware mais recentes e realize uma Análise de Sistema.

Assim que a análise do sistema terminar, selecione a ação pretendida para os itens infetados (Desinfetar, Eliminar, Mover para a Quarentena).

Atenção

Se suspeitar que o ficheiro faz parte do sistema operativo do Windows ou que não é um ficheiro infectado, não siga estes passos e contacte e Apoio ao Cliente do Bitdefender assim que possível.

Se não for possível efetuar a ação selecionada e o relatório da análise indicar uma infecção que não foi possível eliminar, tem de remover o(s) ficheiro(s) manualmente:

O primeiro método pode ser utilizado no modo normal:

1. Desative a proteção antivírus em tempo real do Bitdefender:
   a. Abra a janela de Bitdefender.
   b. Aceda ao painel de **Proteção**.
   c. Clique no módulo **Antivírus**.
   d. Na janela **Antivírus**, selecione o separador **Escudo**.
   e. Clique no botão para desligar **Análise no-acesso**.
2. Mostrar objetos ocultos no Windows. Para saber como fazer isto, consulte "*Como posso mostrar objetos ocultos no Windows?*" (p. 82).
3. Procure a localização do ficheiro infectado (veja no relatório da análise) e elimine-o.
4. Ligue a proteção antivírus em tempo real do Bitdefender.

No caso de o primeiro método falhar ao remover a infecção, siga os seguintes passos:

1. Reinicie o seu sistema e inicie sessão no Modo de Segurança. Para saber como fazer isto, consulte "*Como posso reiniciar no Modo de Segurança?*" (p. 85).
2. Mostrar objetos ocultos no Windows. Para saber como fazer isto, consulte "*Como posso mostrar objetos ocultos no Windows?*" (p. 82).
3. Procure a localização do ficheiro infectado (veja no relatório da análise) e elimine-o.
4. Reinicie o seu sistema e inicie sessão no modo normal.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 227).

33.3. Como posso limpar um vírus num ficheiro?

Um arquivo é um ficheiro ou um conjunto de ficheiros comprimidos num formato especial para reduzir o espaço no disco necessário para armazenar os ficheiros.

Alguns destes formatos são formatos livres, possibilitando ao Bitdefender a opção de analisar o conteúdo e aplicar as ações adequadas para os remover.

Outros formatos de arquivo estão parcial ou totalmente fechados, mas o Bitdefender só pode detetar a presença de vírus no interior, mas não pode aplicar outras ações.

Se o Bitdefender avisar que foi detetado um vírus dentro de um arquivo e não estiver disponível uma ação, significa que não é possível remover o vírus devido a restrições nas definições de permissão do arquivo.

Pode limpar um vírus armazenado num arquivo da seguinte forma:

1. Identifique o ficheiro que contém o vírus realizando uma Análise Completa ao sistema.
2. Desative a proteção antivírus em tempo real do Bitdefender:
   a. Abra a janela de Bitdefender.
   b. Aceda ao painel de **Proteção**.
   c. Clique no módulo **Antivírus**.

d. Na janela **Antivírus**, selecione o separador **Escudo**.

e. Clique no botão para desligar **Análise no-acesso**.

3. Vá à localização do arquivo e descomprima-o com uma aplicação de arquivo, como o WinZip.
4. Identifique e elimine o ficheiro infectado.
5. Elimine o arquivo original de modo a garantir que a infecção é totalmente removida.
6. Comprima novamente os ficheiros num novo arquivo com uma aplicação de arquivo, como o WinZip.
7. Ative a proteção antivírus em tempo real do Bitdefender e execute uma análise completa ao sistema para se certificar que não há outras infecções no sistema.

Nota
É importante saber que um vírus armazenado num arquivo não é uma ameaça imediata ao seu sistema pois o vírus tem de ser descomprimido e executado de modo a infectar o seu sistema.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 227).

33.4. Como posso limpar um vírus num ficheiro do email?

O Bitdefender também pode identificar vírus em bases de dados de correio eletrónico e arquivos de correio eletrónico armazenados no disco.

Por vezes, é necessário identificar a mensagem infectada com a informação fornecida no relatório da análise, e elimine-o manualmente.

Pode limpar um vírus armazenado num arquivo de correio eletrónico da seguinte forma:

1. Analisar a base de dados do correio eletrónico com o Bitdefender.
2. Desative a proteção antivírus em tempo real do Bitdefender:
   a. Abra a janela de Bitdefender.
   b. Aceda ao painel de **Proteção**.

c. Clique no módulo **Antivírus**.

d. Na janela **Antivírus**, selecione o separador **Escudo**.

e. Clique no botão para desligar **Análise no-acesso**.

3. Abra o relatório da análise e utilize a informação de identificação (Assunto, De, Para) das mensagens infectadas para localizá-las no cliente de correio eletrónico.
4. Elimine as mensagens infectadas. A maioria dos clientes de correio eletrónico move a mensagem eliminada para uma pasta de recuperação, a partir da qual pode ser recuperada. Deve certificar-se que a mensagem também é eliminada desta pasta de recuperação.
5. Compactar a pasta com a mensagem infectada.
   - No Outlook Express: No menu Ficheiro, clique em Pasta e, depois em Compactar Todas as Pastas.
   - No Microsoft Outlook 2007: No menu Ficheiro, clique em Gestão de Ficheiros de Dados. Selecione os ficheiros das pastas (.pst) que pretende compactar e clique em Definições. Clique em Compactar Agora.
   - No Microsoft Outlook 2010/2013: No menu Ficheiro, clique em Informações e, em seguida, em definições de Conta (Adicionar e remover contas ou alterar as definições de ligação existentes). Clique em Ficheiro de Dados, selecione os ficheiros das pastas (.pst) que pretende compactar e clique em Definições. Clique em Compactar Agora.
6. Ligue a proteção antivírus em tempo real do Bitdefender.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 227).

33.5. O que fazer se suspeitar que um ficheiro é perigoso?

Pode suspeitar que um ficheiro do seu sistema é perigoso, embora o seu produto Bitdefender não o tenha detetado.

Para se certificar de que o seu sistema está protegido, siga estes passos:

1. Execute uma **Análise de Sistema** com o Bitdefender. Para saber como fazer isto, consulte "*Como posso analisar o seu sistema?*" (p. 61).

2. Se no resultado da análise parece estar limpo, mas você ainda tem dúvidas e quer verificar o ficheiro, contacte os representantes do suporte para que o possamos ajudar.

   Para saber como fazer isto, consulte "*Pedir Ajuda*" (p. 227).

33.6. Como limpar ficheiros infectados da Informação de Volume do Sistema

A pasta de Informação de Volume do Sistema é uma zona no seu disco rígido criada pelo Sistema Operativo e utilizada pelo Windows para armazenar informações essenciais relacionadas com a configuração do sistema.

Os motores do Bitdefender podem detetar qualquer ficheiro infectado armazenado na Informação de Volume de Sistema mas, sendo esta uma área protegida, poderá não conseguir removê-lo.

Os ficheiros infectados detetados nas pastas do Restauro do Sistema aparecerão no relatório da análise da seguinte forma:

?:\Informação de Volume de Sistema_restore{B36120B2-BA0A-4E5D-...

Para remover total e imediatamente o(s) ficheiro(s) infectado(s) do armazém de dados, desative e reative o recurso do Restauro do Sistema.

Se o Restauro do Sistema estiver desativado, todos os pontos de restauro são removidos.

Quando o Restauro do Sistema é novamente ativado, são criados novos pontos de restauro consoante as necessidades do agendamento e de eventos.

Para desativar o Restauro do Sistema, siga os seguintes passos:

- **Para o Windows XP:**

  1. Siga este caminho: **Iniciar** → **Todos os Programas** → **Acessórios** → **Ferramentas do Sistema** → **Restauro do Sistema**
  2. Clique em **Definições do Restauro do Sistema**, no lado esquerdo da janela.
  3. Selecione a caixa de seleção **Desativar Restauro do Sistema** em todas as unidades e clique em **Aplicar**.
  4. Quando receber a notificação que todos os Pontos de Restauro serão eliminados, clique em **Sim** para continuar.

5. Para ativar o Restauro do Sistema, desmarque a caixa de seleção **Desativar Restauro do Sistema** em todas as unidades e clique em **Aplicar**.

- **Para o Windows Vista:**

1. Siga o seguinte caminho: **Iniciar** → **Painel de Controlo** → **Sistema e Manutenção** → **Sistema**
2. No painel da esquerda, clique em **Proteção do Sistema**.

   Se lhe for pedida a palavra-passe de administrador ou a confirmação, escreva a palavra-passe ou dê a confirmação.
3. Para desativar a Restauração do Sistema, desmarque as caixas de seleção de cada unidade e clique em **OK**.
4. Para ativar o Restauro do Sistema, desmarque as caixas de seleção de cada unidade e clique em **OK**.

- **Para o Windows 7:**

1. Clique em **Iniciar**, clique com o botão direito em **Computador** e clique em **Propriedades**.
2. Clique na hiperligação da **Proteção do sistema** no painel da esquerda.
3. Nas opções da **Proteção do Sistema**, selecione a letra de cada unidade e clique em **Configurar**.
4. Selecione **Desativar proteção do sistema** e clique em **Aplicar**.
5. Clique em **Eliminar**, clique em **Continuar** quando pedido e, depois, clique em **OK**.

- **Para o Windows 8:**

1. A partir do ecrã Iniciar do Windows, localize **Computador** (por exemplo, pode começar a digitar "Computador" diretamente no menu Iniciar) e, em seguida, clique no seu ícone.
2. Clique na hiperligação da **Proteção do sistema** no painel da esquerda.
3. Nas opções da **Proteção do Sistema**, selecione a letra de cada unidade e clique em **Configurar**.
4. Selecione **Desativar proteção do sistema** e clique em **Aplicar**.

Se esta informação não o ajudou, poderá contactar a Bitdefender para suporte, como descrito na secção "*Pedir Ajuda*" (p. 227).

33.7. O que são os ficheiros protegidos por palavra-passe no relatório de análise?

Isto é apenas uma notificação que indica que o Bitdefender detetou que estes ficheiros estão protegidos por palavra-passe ou por outra forma de encriptação.

Normalmente, os itens protegidos por palavra-passe são:

- Ficheiros que pertencem a outras solução de segurança.
- Ficheiros que pertencem ao sistema operativo.

Para analisar verdadeiramente os conteúdos, estes ficheiros têm de ser extraídos ou descodificados.

Se estes conteúdos pudessem ser extraídos, o verificador em tempo real do Bitdefender analisaria-os automaticamente para manter o seu computador protegido. Se pretende analisar esses ficheiros com o Bitdefender, terá de contactar o fabricante do produto para receber mais informações sobre esses ficheiros.

Recomendamos que ignore estes ficheiros pois não constituem uma ameaça ao seu sistema.

33.8. O que são os itens ignorados no relatório de análise?

Todos os ficheiros que aparecem como Ignorados no relatório de análise estão limpos.

Para um melhor desempenho, o Bitdefender não analisa ficheiros que não tenham sido alterados desde a última análise.

33.9. O que são os ficheiros muito comprimidos no relatório de análise?

Os itens sobre-comprimidos são elementos que não puderam ser extraídos pelo motor de análise ou elementos para os quais a desencriptação levaria demasiado tempo, tornando o sistema instável.

Sobre-comprimido significa que o Bitdefender não realizou a análise a esse arquivo pois a descompactação iria consumir demasiados recursos do

sistema. O conteúdo será analisado aquando o acesso em tempo real, se necessário.

33.10. Por que é que Bitdefender eliminou automaticamente um ficheiro infectado?

Se for detetado um ficheiro infectado, o Bitdefender tentará automaticamente desinfectá-lo. Se a desinfecção falhar, o ficheiro é movido para a quarentena de modo a restringir a infecção.

Para determinados tipos de malware, a desinfecção não é possível por o ficheiro detectado ser totalmente malicioso. Nestes casos, o ficheiro infectado é eliminado do disco.

Este é, normalmente, o caso de ficheiros de instalação que são transferidos de sites Internet suspeitos. Se se deparar numa situação assim, transfira o ficheiro de instalação do site Internet do fabricante ou de outro site fidedigno.

CONTACTE-NOS

34. PEDIR AJUDA

O Bitdefender fornece aos seus clientes um nível de suporte rápido e eficaz. Se encontrar algum problema ou se tiver alguma questão sobre o nosso produto Bitdefender, pode utilizar vários recursos online para encontrar uma solução ou resposta. Ou, se preferir, poderá contactar a equipa de Suporte ao Cliente do Bitdefender. Os nossos técnicos de apoio responderão atempadamente às suas questões e dar-lhe-ão a ajuda que precisar.

A secção "*Resolver incidências comuns*" (p. 190) fornece as informações necessárias relativamente às incidências mais frequentes que poderá encontrar ao utilizar este produto.

Se não encontrar a resposta à sua pergunta nos recursos disponibilizados, pode contactar-nos diretamente:

- "Contacte-nos diretamente do seu produto Bitdefender" (p. 227)
- "Contacte-nos através do nosso Centro de Suporte Online" (p. 228)

Importante
Para contactar o Apoio ao Cliente da Bitdefender tem de registar o seu produto Bitdefender. Para mais informação, por favor consulte o "*A registar o Bitdefender*" (p. 39).

Contacte-nos diretamente do seu produto Bitdefender

Se possuir uma ligação ativa à Internet, pode contactar o apoio do Bitdefender diretamente a partir da interface do produto.

Siga os seguintes passos:

1. Abra a janela de Bitdefender.
2. Clique no ícone na parte superior da janela e selecione **Ajuda & Suporte** no menu suspenso.
3. Tem as seguintes opções:
   - **Documentação do Produto**

     Aceda à nossa base de dados e procure a informação necessária.
   - **Contato de Suporte**

     Utilize o botão **Contatar Suporte** para executar a Ferramenta de Suporte do Bitdefender e contatar o Departamento de Apoio ao Cliente. Pode

navegar pelo assistente utilizando o botão **Seguinte**. Para sair do assistente, clique em **Cancelar**.

a. Selecione a caixa de verificação para indicar aceitação e clique em **Seguinte**.

b. Complete o formulário de envio com os dados necessários:

   i. Insira o seu endereço de email.

   ii. Digite o seu nome completo.

   iii. Introduza a descrição do problema que encontrou.

   iv. Marque a opção **Tentar reproduzir a incidência antes de enviar** caso esteja a encontrar uma incidência do produto. Continue com os passos necessários.

c. Por favor, aguarde alguns minutos enquanto o Bitdefender recolhe as informações relacionadas com o produto. Esta informação irá ajudar os nossos engenheiros a encontrar uma solução para o seu problema.

d. Clique em **Concluir** para enviar as informações ao Departamento de Apoio ao Cliente da Bitdefender. Será contactado assim que possível.

Contacte-nos através do nosso Centro de Suporte Online

Se não conseguir aceder às informações necessárias com o produto Bitdefender, por favor consulte o nosso Centro de Suporte online:

1. Vá para http://www.bitdefender.pt/support/consumer.html.

   O Centro de Suporte da Bitdefender possui inúmeros artigos que contêm soluções para incidências relacionadas com o Bitdefender.

2. Utilize a barra de pesquisa na parte superior da janela para encontrar artigos que possam fornecer uma solução definitiva para o seu problema. Para pesquisar, basta digitar o termo na barra de pesquisa e clicar em **Pesquisar**.

3. Leia os artigos ou os documentos e experimente as soluções propostas.

4. Se a solução não resolver o seu problema, aceda a

   http://www.bitdefender.pt/support/contact-us.htmle contate os nossos representantes do suporte.

35. RECURSOS ONLINE

Estão disponíveis vários recursos online para o ajudar a resolver problemas e a responder a questões relacionados com o Bitdefender.

- Centro de Suporte Bitdefender:

  http://www.bitdefender.pt/support/consumer.html

- Fórum de Suporte Bitdefender:

  http://forum.bitdefender.com

- o portal de segurança informática HOTforSecurity:

  http://www.hotforsecurity.com

Também pode utilizar o seu motor de busca favorito para saber mais sobre a segurança de computadores, os produtos Bitdefender e a empresa.

35.1. Centro de Suporte Bitdefender

O Centro de Suporte do Bitdefender é um repositóio de informação online sobre os produtos Bitdefender. Armazena, num formato facilmente acessível, apresenta relatórios sobre os resultados do suporte técnico em curso e atividades de correção de falhas do suporte e equipas de desenvolvimento do Bitdefender, para além de artigos mais gerais sobre prevenção d vírus, a gestao de soluções do Bitdefender com explicações detalhadas e muitos outros artigos.

O Centro de Suporte da Bitdefender está aberto ao público e é pesquisável. A informção extensiva que contém é mais um meio de proporcionar aos clientes do Bitdefender informações técnicas e conhecimento de que necessitam. Todos os pedidos válidos de informação ou relatórios de falhas oriundos de clientes do Bitdefender são eventualmente direcionados para o Centro de Apoio do Bitdefender, como relatórios de correção de falhas, fichas de resolução de problemas ou artigos informacionais como suplemento dos ficheiros de ajuda.

O Centro de Suporte da Bitdefender encontra-se disponível a qualquer altura

http://www.bitdefender.pt/support/consumer.html.

35.2. Fórum de Suporte Bitdefender

O Fórum de Suporte do Bitdefender proporciona aos utilizadores do Bitdefender uma forma fácil de obter ajuda e ajudar os outros.

Se o seu produto Bitdefender não estiver a funcionar corretamente, se não conseguir remover certos vírus do seu computador ou se tiver alguma questão sobre a forma como opera, coloque o seu problema ou a sua questão no fórum.

Os técnicos de apoio da Bitdefender supervisionam o fórum, à espera de novas mensagens para fornecer ajuda. Também pode receber uma resposta ou solução de um utilizador mais experiente do Bitdefender.

Antes de publicar o seu problema ou questão, por favor pesquise o fórum por um tópico semelhante ou relacionado.

O Fórum de Suporte do Bitdefender está disponível em http://forum.bitdefender.com, em 5 idiomas diferentes: inglês, alemão, francês, espanhol e romeno. Clique na hiperligação **Proteção Casa & Casa/Escritório** para aceder à secção dedicada aos produtos de consumidor.

35.3. Portal HOTforSecurity

HOTforSecurity é uma fonte rica de informações sobre segurança de computadores. Aqui, pode ficar a conhecer as várias ameaças a que o seu computador fica exposto quando ligado à Internet (malware, phishing, spam, cibercriminosos).

Os novos artigos são publicados regularmente para o manter atualizado sobre as últimas ameaças descobertas, as atuais tendências de segurança e outras informações sobre a indústria de segurança informática.

A página web do HOTforSecurity é http://www.hotforsecurity.com.

36. INFORMAÇÃO DE CONTACTO

Comunicação eficiente é a chave de um negócio bem-sucedido. Durante os últimos 10 anos a BITDEFENDER estabeleceu uma reputação indiscutível ao exceder as expectativas dos clientes e parceiros, ao procurar constantemente melhorar a comunicação. Por favor não hesite em contactar-nos acerca de qualquer questão ou assunto que nos queira colocar.

36.1. Endereços Web

Departamento Comercial: comercial@bitdefender.pt
Centro de Suporte:http://www.bitdefender.pt/support/consumer.html
Documentação: documentation@bitdefender.com
Distribuidores locais:http://www.bitdefender.pt/partners
Programa de parcerias: partners@bitdefender.com
Relações com os media: pr@bitdefender.com
Carreiras: jobs@bitdefender.com
Submeter Vírus: virus_submission@bitdefender.com
Submeter Spam: spam_submission@bitdefender.com
Relatórios de Abusos: abuse@bitdefender.com
Site Web:http://www.titaniumwalls.pt

36.2. Distribuidores locais

Os distribuidores locais Bitdefender estão preparados para responder a quaisquer dúvidas relacionadas com as suas áreas de operação, quer sejam comerciais ou assuntos gerais.

Para encontrar um distribuidor Bitdefender no seu país:

1. Vá para http://www.bitdefender.pt/partners/#Partner Locator/.
2. Clique no separador **Localizador de Parceiros**.
3. A informação de contacto dos distribuidores locais Bitdefender deve ser automaticamente apresentada. Se isto não acontecer, selecione o país em que reside para visualizar a informação.
4. Se não encontrar um distribuidor Bitdefender no seu país, não hesite em contactar-nos por correio eletrónico através do endereço sales@bitdefender.com. Por favor, escreva a sua mensagem em inglês para podermos responder imediatamente.

36.3. Escritórios Bitdefender

Os escritórios locais Bitdefender estão preparados para responder a quaisquer dúvidas relacionadas com as suas áreas de operação, quer sejam comerciais ou assuntos gerais. Os seus respectivos endereços e contactos estão listados abaixo.

E.U.A.

Bitdefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
Telefone (office&sales): 1-954-776-6262
Vendas: sales@bitdefender.com
Suporte Técnico: http://www.bitdefender.com/support/consumer.html
Web: http://www.bitdefender.com

UK e Irlanda

Genesis Centre Innovation Way
Stoke-on-Trent, Staffordshire
ST6 4BF
Endereço eletrónico: info@bitdefender.co.uk
Tel: +44 (0) 8451-305096
Vendas: sales@bitdefender.co.uk
Suporte Técnico: http://www.bitdefender.com/support/consumer.html
Web: http://www.bitdefender.co.uk

Alemanha

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
Deutschland
Escritório: +49 2304 9 45 - 162
Fax: +49 2304 9 45 - 169
Vendas: vertrieb@bitdefender.de
Suporte Técnico: http://www.bitdefender.de/support/consumer.html
Web: http://www.bitdefender.de

Espanha

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Fax: +34 93 217 91 28
Tel: +34 902 19 07 65
Vendas: comercial@bitdefender.es
Suporte Técnico: http://www.bitdefender.es/support/consumer.html
Website: http://www.bitdefender.es

Roménia

BITDEFENDER SRL
Complex DV24, Building A, 24 Delea Veche Street, Sector 2
Bucharest
Fax: +40 21 2641799
Telefone Comercial: +40 21 2063470
E-mail Vendas: sales@bitdefender.ro
Suporte Técnico: http://www.bitdefender.ro/support/consumer.html
Website: http://www.bitdefender.ro

United Arab Emirates

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Telefone Comercial: 00971-4-4588935 / 00971-4-4589186
E-mail Vendas: sales@bitdefender.com
Suporte Técnico: http://www.bitdefender.com/support/consumer.html
Website: http://www.bitdefender.com/world

Glossário

ActiveX

O ActiveX é um modelo para fazer programas de forma a que outros programas e o sistema operativo os possam chamar. A tecnologia do ActiveX é usada com o Microsoft Internet Explorer para criar páginas da Web interactivas, que parecem e comportam-se como programas de computador, em vez de páginas estáticas. Com o ActiveX, os utilizadores podem efectuar perguntas ou responder a questões, usando botões para carregar, e interagir de outras formas com a página da Web. Os controlos do ActiveX são frequentemente escritos utilizando o Visual Basic.

O Active X é notável para um leque completo de controlos de segurança; os especialistas de segurança dos computadores desencorajam o seu uso na Internet.

Adware

O adware é com frequência combinado com uma aplicação hospedeira que é fornecida sem custo desde que o utilizador concorde em aceitar o adware. Por causa das aplicações adware serem normalmente instaladas após o utilizador concordar com uma licença de uso que define o propósito da aplicação, nenhuma ilegalidade é na verdade cometida.

No entanto, anúncios tipo pop-up podem tornar-se bastante incomodativos, e em alguns casos podem mesmo degradar a performance do sistema. Também, a informação que algumas dessas aplicações recolhem podem causar algumas preocupações de privacidade aos utilizadores que não estão completamente conscientes dos termos da licença de uso.

Arquivo

Um disco, cassete, ou diretório que contém ficheiros que foram armazenados.

Um ficheiro que contém um ou mais ficheiros num formato comprimido.

Assinatura de Vírus

A patente binária de um vírus, usada pelo programa de anti-vírus para detetar e eliminar os vírus.

Atualização

Uma nova versão de um produto de software ou hardware desenhada para substituir uma versão antiga do mesmo produto. Em adição, a instalação de rotina da actualização verifica se a versão anterior já está instalada no seu computador; se não estiver, não poderá instalar a actualização.

O Bitdefender tem o seu próprio modulo de atualização que lhe permite verificar atualizações manualmente, ou permitir atualizar o produto automaticamente.

Caixa do sistema

Introduzido com o Windows 95, o tabuleiro do sistema está localizado na barra de tarefas do Windows (normalmente em baixo, junto ao relógio) e contém ícones em miniatura para um acesso fácil às funções do sistema, tais como fax, impressora, modem, volume, etc. Faça duplo-clique ou clique com o botão direito sobre o ícone para ver e aceder aos detalhes e controlos.

Caminho

As direcções exactas para um ficheiro num computador. Estas direções são normalmente descritas por meios de preenchimento hierárquico do topo para baixo.

A rota entre dois dados pontos, tal como os canais de comunicação entre dois.

Cliente de mail

Um cliente de e-mail é uma aplicação que lhe permite enviar e receber e-mail.

Componente (drive) do disco

É uma máquina que lê os dados do disco e escreve dados num disco.

Uma componente de disco rígido lê e escreve discos rígidos.

Uma componente de disquetes acede às disquetes.

As componentes do disco tanto podem ser internas (dentro do computador) ou externas (vêm numa caixa em separado que se liga ao computador).

Cookie

Dentro da indústria da Internet, as cookies são descritas como pequenos ficheiros, que contêm informação acerca de computadores individuais, que podem ser analizados e usados pelos publicitários para seguir o rasto online do seus interesses e gostos. Neste domínio, a tecnologia das cookies ainda está a ser desenvolvida e a sua intenção é procurar atingi-lo com publicidade naquilo que disse serem os seus interesses. É uma espada de dois gumes para muitas pessoas, porque, por um lado é eficiente e pertinente já que apenas vê anúncios do seu interesse. Por outro lado, envolve realmente "seguir o rasto" e "perseguir" onde vai e no que clica. Compreensivelmente, existe um debate acerca da privacidade e muitas pessoas sentem-se ofendidas ao terem a noção que estão a ser vistas como um "número SKU " (sabe, o código de barras por detrás das embalagens que é verificado na mercearia). Apesar deste ponto de vista parecer ser extremo, em alguns casos é exacto.

Download

Para copiar dados (normalmente um ficheiro interno) de uma fonte principal para um aparelho periférico. O termo é frequentemente utilizado para descrever o processo de copiar um ficheiro de um serviço online para o seu próprio computador. O download também se pode referir à cópia de um ficheiro de um servidor de ficheiros de rede, para um computador na rede.

E-mail

Correio electrónico. É um serviço que envia mensagens de computadores via redes locais ou globais.

Escrita

Outro termo para macro ou ficheiro de porção, uma escrita é uma lista de comandos que podem ser executados sem a interação do utilizador.

Eventos

Uma ação ou ocorrência detetada por um programa. Os eventos podem ser ações do utilizador, tais como clicar no botão do rato ou carregar numa tecla, ou ocorrências do sistema, tal como ficar sem memória.

Extensão do nome do ficheiro

A porção de um nome de ficheiro, que segue o ponto final, a qual indica o tipo de dados armazenados no ficheiro.

Muitos sistemas operativos usam extensões do nome do ficheiro, por ex. Unix, VMS, e MS-DOS. Elas são normalmente de uma a três letras (alguns SOs antigos não suportam mais do que três). Os exemplos íncluem ".c" para C de código da fonte, ".ps" para PostScript, ".txt" para texto arbitrário.

Falso positivo

Ocorre quando o verificador identifica um ficheiro como infectado, quando na verdade ele não está.

Ficheiro de reporte

Um ficheiro que lista acções que ocorreram. O Bitdefender um ficheiro de reporte que lista o caminho examinado, as pastas, o número de arquivos e ficheiros examinados, e quantos ficheiros suspeitos e infectados foram encontrados.

Heurístico

Um método baseado em regras de identificação de novos vírus. Este método de análise não se baseia em assinaturas específicas de vírus. A vantagem da análise heurística, é que não se deixa enganar por uma nova variante de um vírus existente. Contudo, pode reportar ocasionalmente códigos suspeitos em programas normais, gerando o chamado "falso positivo".

IP

Internet Protocol - Um rótulo de protocolo no protocolo TCP/IP séquito que é responsável dos endereços de IP, rotas, e a fragmentação e reabertura dos pacotes de IP.

Itens de Arranque

Qualquer ficheiro colocado nesta pasta, irá abrir quando o computador iniciar. Por exemplo, um ecrã que abra no ínicio, um ficheiro de som a ser tocado quando ligar inicialmente o computador, um lembrete, ou programas de aplicação podem ser itens que começam a funcionar ao iniciar o computador. Normalmente, é colocado um pseudónimo deste ficheiro nesta pasta, em vez do ficheiro em si.

Java applet

Um programa em Java é desenhado para funcionar apenas numa página web. Para usar uma applet numa página web, deverá especificar o nome da applet e o tamanho (comprimento e largura - em pixels) que a applet

pode utilizar. Quando a página da web é acedida, o motor de busca descarrega a applet de um servidor e executa-a na máquina do utilizador (o cliente). As applets diferem das aplicações, pois são administradas por um protocolo de segurança restrito.

Por exemplo, apesar de as applets se executarem no cliente, elas não podem escrever nem ler dados na máquina do cliente. Adicionalmente, as applets são restritas para que possam apenas ler e escrever dados provenientes do mesmo domínio do qual elas são servidas.

Keylogger

Um keylogger é uma aplicação que regista tudo o que digita.

Os keyloggers não são por natureza maliciosos. Podem ser usados com objectivos legítimos, tais como monitorizar a actividade de funcionários ou das crianças. No entanto, são cada vez mais usados por cibercriminosos com objectivos maliciosos (por exemplo, para recolher dados privados, tais como credenciais de acesso e números da segurança social).

Linha de comando

Numa interface de linha do comando, o utilizador introduz comandos no espaço providenciado diretamente no ecrã, usando a linguagem de comando.

Macro vírus

Um tipo de vírus de computador que está codificado como uma macro retido num documento. Muitas aplicações, tais como Microsoft Word e Excel, contêm poderosas linguagens macro.

Estas aplicações permitem-lhe reter uma macro num documento, e ter a macro pronta a ser executada sempre que o documento for aberto.

Memória

Áreas internas de armazenamento no computador. O termo memória identifica armazenamento de dados que vêm na forma de chips, e a palavra armazenar é usada para a memória que existe em cassetes ou discos. Todo o computador vem com uma certa quantidade de memória física, normalmente referida como memória principal ou RAM.

Minhoca
Um programa que se propaga a si próprio ao longo de uma rede, reproduzindo-se à medida que avança. Não pode ligar-se sozinho a outros programas.

Não-heurístico
Este método de análise depende da assinaturas de vírus especificas. A vantagem de uma análise não-heurística, é que ela não será induzido em erro pelo que possa parecer um vírus e não gera falsos alarmes.

Navegador
É um software de aplicação usado para localizar e mostrar páginas da Web. Os navegadores mais populares são o Microsoft Internet Explorer, Mozilla Firefox e Google Chrome. Estes são motores de busca gráficos, o que significa que eles tanto podem mostrar gráficos como texto. Em adição, a maioria dos motores de busca modernos podem apresentar informação multimédia, incluíndo som e vídeo, apesar de requererem plug-ins para alguns formatos.

Phishing
O acto de enviar um e-mail a um utilizador como sendo falsamente uma empresa legítima e estabelecida numa tentativa de levar o utilizador a providenciar informação privada que será utilizada para roubo. O e-mail leva o utilizador a visitar um site na Internet onde lhe é solicitado que actualize informação pessoal, tal como palavras-passe e números de cartões de crédito, segurança social, e números de contas bancárias, que a legítima organização já possui. O site web, no entanto, é falso e está feito apenas para roubar a informação ao utilizador.

Photon
Photon é uma tecnologia inovadora não-intrusiva da Bitdefender, desenhado para minimizar o impacto da proteção antivírus no desempenho. Ao monitorizar a atividade do seu PC em segundo plano, ele cria padrões de utilização que ajudam a otimizar os processos de arranque e de análise.

Porta
Uma interface num computador, à qual se liga um dispositivo. Os computadores pessoais têm vários tipos de portas. Internamente, existem várias portas para ligar as drives de disco, ecrãs, e teclados.

Externamente, os computadores pessoais têm portas para ligar modems, impressoars, ratos, e outros dispositivos periféricos.

Nas redes TCP/IP e UDP, um ponto final para uma ligação lógica. O número da porta identifica que tipo de porta se trata. Por exemplo, a porta 80 é usada para o tráfego HTTP.

Porta das traseiras

Um buraco na segurança de um sistema deliberadamente criado pelos desenhadores ou responsáveis da manutenção. A motivação para tais buracos não é sempre sinistra; alguns sistemas operativos, por exemplo, que trazem contas privilegiadas, criadas para serem usadas pelos técnicos de serviço ou pelo vendedor dos programas de manutenção.

Programas compactados

Um ficheiro num formato compactado. Muitos sistemas operativos e aplicações contêm comandos que lhe permitem compactar um ficheiro, para que ocupe menos memória. Por exemplo, suponha que tem um ficheiro de texto contendo dez espaços de caracteres consecutivos. Normalmente, isto iria requerer dez bytes de armazenamento.

Contudo, um programa que compacta ficheiros iria substituir o espaço dos caracteres por uma série-de-espaços de caracteres especial, seguida pelo número de espaços a serem substituidos. Neste caso, os dez espaços iriam requerer apenas dois bytes. Esta é apenas uma técnica de compactar - existem muitas mais.

Rootkit

Um rootkit é um pacote de ferramentas de software que proporcionam um nível de acesso de administrador a um sistema. O termo foi usado em primeiro lugar nos sistemas operativos UNIX e referia-se a ferramentas recompiladas que proporcionavam aos intrusos direitos de administração, permitindo-lhes ocultar a sua presença de forma a não serem vistos pelos administradores do sistema.

O papel principal dos rootkits é ocultar processos, ficheiros, logins e registos. Eles também podem intercetar dados dos terminais, ligações de rede ou periféricos, se eles incorporarem o software para tal.

Os rootkits não são maliciosos por natureza. Por exemplo, os sistemas e mesmo algumas aplicações ocultam ficheiros críticos usando rootkits. No entanto, eles são essencialmente utilizados para ocultar malware

ou para esconder a presença de um intruso no sistema. Quando combinados com o malware, os rootkits são uma grande ameaça à integridade e segurança de um sistema. Eles podem monitorizar tráfego, criar backdoors no sistema, alterar ficheiros e relatórios e evitarem ser detetados.

Sector de saída

Um sector no início de cada disco que identifica a arquitectura do disco (tamanho do sector, tamanho do grupo, e por aí fora). Para discos de inicialização, o sector de saída também contém um programa que carrega o sistema operativo.

Spam

Lixo de correio electrónico ou lixo de avisos de newsgroups. É normalmente conhecido como correio não-solicitado.

Spyware

Qualquer software que encobertamente reune informação do utilizador através da ligação à Internet do utilizador sem o seu conhecimento, normalmente para propósitos de publicidade. As aplicações de spyware são tipicamente adicionadas como um elemento oculto de programas freeware ou shareware que podem ser download a partir da Internet; no entanto salientamos que a maioria das aplicações freeware ou shareware não possuem spyware. Uma vez instalado, o spyware monitoriza a actividade do utilizador na Internet e transmite essa informação em background para alguém. O spyware pode também reunir informação acerca de endereços de e-mail e até mesmo palavras-passe e números de cartões de crédito.

O spyware é similar a um cavalo-de-troia em que os utilizadores o instalam sem saberem, enquanto estão a instalar outra coisa qualquer. Uma forma comum de ser uma vítima de spyware é fazer download de determinado ficheiro peer-to-peer de produtos de swapping que se encontram actualmente disponíveis.

Para além destas questões de ética e privacidade, o spyware priva o utilizador de recursos de memória e também de largura de banda pois para enviar informação do utilizador para a fonte do spyware usa a ligação à Internet do utilizador. Por causa do spyware utilizar memória e recursos do sistema, as aplicações que estão a funcionar em

background podem causar crashes no sistema ou uma grande instabilidade geral.

TCP/IP

Transmission Control Protocol/Internet Protocol - Um conjunto de protocolos de uma rede de trabalho abrangentemente usados Internet que permite comunicações ao londo de redes de computadores interconectadas com várias arquitecturas de hardware e vários sistemas operaticos. O TCP/IP ínclui padrões de como os computadores comunicam e convenções para ligar redes e conduzir o tráfego.

Tróiano

Um programa destrutivo que se mascara de aplicação benigna. Ao contrário dos vírus, os cavalos de Tróia não se replicam, mas podem ser tão destrutivos como os vírus. Um dos cavalos de Tróia mais insidiosos é o programa que promete ver-se livre dos vírus do seu computador, mas em vez disso introduz vírus no seu computador.

O termo provém de uma história da Ilíada de Homero, na qual os Gregos deram um cavalo gigante de Madeira aos seus inimigos, os Troianos, como uma oferta majestosa. Mas após os Troianos levarem o cavalo para dentro das muralhas da sua cidade, os soldados Gregos saíram para fora do cavalo e abriram os portões da cidade, permitindo que os seus compatriotas entrassem e dominassem Tróia.

Vírus

Um programa ou um pedaço de código que é carregado no seu computador sem o seu conhecimento e executa-se contra a sua vontade. A maioria dos vírus podem-se replicar. Todos os vírus de computação são feitos pelo Homem. Um simples vírus que se possa reproduzir a si próprio vezes sem conta, é relativamente fácil de fabricar. Mesmo um simples vírus é perigoso, porque usará rapidamente toda a memória disponível e levará o sistema a uma quebra. Um tipo de vírus ainda mais perigoso é aquele que é capaz de se transmitir ao longo das redes e ultrapassar sistemas de segurança.

Vírus de saída

Um vírus que infecta o sector boot de um disco fixo ou de uma unidade de disquetes. A tentativa de arrancar por uma disquete infectada por um vírus de boot, irá causar a activação do vírus em memória. Sempre

que iniciar o seu sistema a partir daquele ponto, terá o vírus activo em memória.

Vírus polimórfico

Um vírus que altera a sua forma a cada ficheiro que infecta. Dado que eles não têm uma padrão de patente binária consistente, tais vírus são difíceis de identificar.